New and Changed Information for Cisco Unified Communications Manager, Release 9.0(1)

First Published: July 18, 2012

Last Modified: July 18, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27435-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Introduction** 1

CHAPTER 2 **Installation, upgrade, and migration** 3

- Installation 3
- Upgrade 3
  - Software version restrictions 3
  - Upgrade order 4
    - Standard upgrade order 4
    - Refresh upgrade order 4
- Migration 5

CHAPTER 3 **New features** 7

- AS-SIP Line Endpoints 8
  - Procedures 13
    - Set up AS-SIP line endpoints 13
  - CLI changes 14
    - No changes. 14
- Avatar device type 14
  - CSF settings information 20
  - CLI changes 37
    - No changes. 37
- Binary Floor Control Protocol, Real-Time Transport Control Protocol, and Far End Camera Control 37
  - CLI changes 39
    - No changes. 39
- Codec preferences 39
  - Procedures 40
    - Create new Audio Codec Preference list 40

Edit Audio Codec Preference list 40
Delete Audio Codec Preference list 41
CLI changes 41
No changes. 41
Confirmed Answer and DVO VM detection 41
CLI changes 44
No changes. 44
CTI support for Native Call Queuing 44
CLI changes 45
No changes. 45
Enhanced E911 support 45
Procedures 46
Set up E911 Messages 46
CLI changes 46
No changes. 46
Enhanced Location Call Admission Control 46
Additional information 52
Enhanced Location Call Admission Control feature 52
Enhanced Location Call Admission Control architecture 55
Location Bandwidth service parameters 59
Shadow system location 59
Devices that support Enhanced Location Call Admission Control 60
Enhanced Call Admission Control limitations 60
Procedures 60
Configure Enhanced Location Call Admission Control 60
CLI changes 61
No changes. 61
Enterprise Licensing Manager 61
CLI changes 62
license management 62
license management change user 62
license management list users 63
Fixed Mobile Convergence (FMC) over SIP trunks without Smart Client 63
CLI changes 65
No changes. 65

G.Clear support for BRI interfaces 65
CLI changes 66
No changes. 66
Hunt Pilot connected number 66
CLI changes 67
No changes. 67
HuntList connected number CTI support 67
CLI changes 68
No changes. 68
HCS Anonymous Call Rejection ISC Trunks 68
CLI changes 70
No changes. 70
HCS supplementary services for VoLTE IMS mobile device 70
CLI changes 74
No changes. 74
IM and Presence service consolidated administration 74
CLI changes 76
No changes. 76
Multiple syslog destination 76
CLI changes 77
No changes. 77
Native Call Queueing on CUCM 77
CLI changes 88
No changes. 88
NextGen mobile clients with QoE 88
CLI changes 89
No changes. 89
Originally Called Party Name in Placed Call History 89
CLI changes 91
No changes. 91
Pause in speed dials 91
CLI changes 92
No changes. 92
Record Line Key 92
Procedures 101

Set up Monitoring and Recording 101
Add the Record softkey or programmable line key to the device template (optional) 101
Enable recording for a line appearance 102
Additional information 102
CLI changes 103
No changes. 103
Secure Adhoc Conference MCU Setup 103
Procedures 104
Set up TLS connection with Cisco TelePresence MCU 104
CLI changes 105
No changes. 105
Secure Cross Cluster Extension Mobility 105
CLI changes 108
No changes. 108
Serviceability for locations CAC enhancements 108
Procedures 110
View locations topology 110
View locations discrepancy 111
View effective path 112
View disconnected groups 112
CLI changes 113
No changes. 113
Session Trace enhancement 113
Procedures 114
Open from local disk 114
CLI changes 116
No changes. 116
SIP CLI handling change 116
CLI changes 118
No changes. 118
SIP Diversion Counter 118
CLI changes 120
No changes. 120
SIP normalization and transparency 120

CLI changes 121
No changes. 121
Single step IP and hostname changes in CUCM cluster 121
CLI changes 128
No changes. 128
SNMP and billing setup using syslog destination address 128
CLI changes 128
No changes. 128
URI dialing and Intercluster Lookup Service 128
Additional information for URI dialing 134
Directory URI format 134
Directory URI provisioning 135
Directory URI and directory number dial string interpretation 135
Directory URI call routing 136
Directory URI interoperability with VCS or third party system 136
Directory URI LDAP integration 137
Directory URI and directory number blended address 138
Directory URI Replication with ILS 139
ILS cluster discovery 140
ILS network components 141
Procedures 142
Set up URI dialing 142
Set up ILS network 143
Set up digit transformations for URI dialing 144
Import Directory URIs from a non-ILS system 145
CLI changes 146
utils ils findroutestring 146
utils ils findxnode 147
utils ils lookup 147
utils ils showpeerinfo 148
User Options page enhancements 148
CLI changes 149
No changes. 149
Video for SNR call 149
Procedures 151

CLI changes 151
Video over Wi-Fi 151
CLI changes 152
No changes. 152
XML Axis framework 2.0 update 152
CLI changes 153
No changes. 153
2000 character LDAP filter size 153
CLI changes 154
No changes. 154

CHAPTER 4 Cisco Unified IP Phones 155
Cisco Unified IP Phones 155
Cisco Unified IP Phone 6900 Series features 156
Device Invoked Recording 156
Extension Mobility Cross Cluster Enhancement 157
Headset Sidetone Control 157
Line Status for Call Lists 158
PLK Support for Queue Statistics 158
Ring Cadence Localization 159
RTCP Behavior On Hold 160
View Call Logs From Shared Line 160
Cisco Unified IP Phone 7900 Series features 160
Device Invoked Recording 161
Extension Mobility Cross Cluster Enhancement 162
Headset Recording 163
HTTP Firmware Upgrade 164
PLK Support for Queue Statistics 165
RTCP Behavior On Hold 165
Secure Extension Mobility Cross Cluster 166
Cisco Unified IP Phone 8941 and 8945 features 167
Call Log Filter Enhancement 167
Device Invoked Recording 168
Extension Mobility Cross Cluster Enhancement 168
Headset Sidetone Control 168

Line Status for Call Lists 169
Pause In Speed Dial 169
PLK Support for Queue Statistics 170
RTCP Control for Video 171
sRTP Secure Video 171
SIP Phone No Alert Name 172
Secure Extension Mobility Cross Cluster 172
Video Disable 173
Cisco Unified IP Phone 8961, 9951, and 9971 features 174
Assured Services SIP 174
Device Invoked Recording 175
Display Survivable Remote Site Telephony Message 175
Edit Speed Dial Without Restart 176
Extension Mobility Cross Cluster Enhancement 176
Handset Audio Tuning 177
Handset Bass Adjustment 177
Pause In Speed Dial 177
PLK Support for Queue Statistics 178
RTCP Hold On SIP 178
RTCP Control for Video 179
Secure Extension Mobility Cross Cluster 179
Simplified New Call Bubble 180
SIP Phone No Alert Name in Placed Calls History 180
sRTP Secure Video 181
Unique Call ID Display 181
Uniform Resource Identifier Dialing 182

CHAPTER 5 Other changes 185

CHAPTER 1

Introduction

This document lists the new features, and changes to existing features, for Cisco Unified Communications Manager 9.0. The features are listed alphabetically. Each section includes:

- a conceptual overview of the feature
- functional area impacts
- CLI impacts
- procedure impacts

CHAPTER 2

Installation, upgrade, and migration

This section contains information about the following topics:

- Installation, page 3
- Upgrade, page 3
- Migration, page 5

Installation

No changes.

For more information, see *Installing Cisco Unified Communications Manager, Release 9.0(1)*.

Upgrade

This section contains the steps to upgrade Unified CM and IM and Presence properly. Depending on your server setup, you can perform a standard or refresh upgrade.

Software version restrictions

From Release 9.0(1) onward, Cisco Unified Communications Manager (Unified CM) and IM and Presence Service software versions must match. For two software versions to match, they must have the same major and minor release number. Major and minor release numbers are defined as follows:

`9.x.y`

where `9` = major release number, `x` = minor release number and `y` = maintenance release number.

For example, IM and Presence Release 9.0.2.10000-4 is compatible with Unified CM Release 9.0.12.30000-2, but it is not compatible with Unified CM Release 9.1.1.10000-3. Similarly, Unified CM Release 8.6.2.10000-6 is not compatible with IM and Presence Release 9.0.1.10000-9.

Note You cannot upgrade IM and Presence to Release 9.0(1) unless Unified CM is running Release 9.0(1) on the active or inactive partition. You must upgrade Unified CM before you can upgrade IM and Presence to the matching version.

Caution If you use Platform Administrative Web Services (PAWS) Management to upgrade IM and Presence, do not attempt to upgrade and reboot to IM and Presence Release 9.0(1) if the active partition on Unified CM is running an incompatible software version. If you do, the upgrade will fail, as expected, but the failure will not be reported until near the end of the upgrade process. You will also experience system downtime when the system reboots.

The delayed upgrade failure notification applies only to upgrades that are performed with PAWS Management. If you perform the upgrade through Cisco Unified IM and Presence Operating System Administration or through the CLI, the upgrade failure notification is displayed at the beginning of the upgrade.

Upgrade order

Note The order in which you upgrade Unified CM and IM and Presence is very important.

Standard upgrade order

The following upgrade paths are standard upgrades:

- Unified CM Release 8.6.x to Unified CM Release 9.0(1)
- Cisco Unified Presence Release 8.6(4) to IM and Presence Service Release 9.0(1)

For standard upgrades, you must perform the upgrades in the following order:

1. Upgrade the Unified CM publisher node.
2. Upgrade the IM and Presence publisher node and the Unified CM subscriber nodes.
3. Upgrade the IM and Presence subscriber nodes.
4. Switch versions on the Unified CM publisher node.
5. Switch versions on the IM and Presence publisher node and Unified CM subscriber nodes.
6. Switch versions on the IM and Presence subscriber nodes.

Refresh upgrade order

The following upgrade paths are refresh upgrades:

- Unified CM Release 8.5 and earlier to Unified CM Release 9.0(1)

- Cisco Unified Presence Release 8.6(3) and earlier to IM and Presence Service Release 9.0(1)

For refresh upgrades, you must perform the upgrades in the following order:

1. Upgrade the Unified CM publisher node
2. Switch versions on the Unified CM publisher node.
3. Upgrade the IM and Presence publisher node and the Unified CM subscriber nodes.
4. Switch versions on the IM and Presence publisher node and Unified CM subscriber nodes.
5. Upgrade the IM and Presence subscriber nodes.
6. Switch versions on the IM and Presence subscriber nodes.

Note Refresh upgrades for Unified CM are described in the topic "Software upgrade process overview" in the *Upgrade Guide for Cisco Unified Communications Manager, Release 9.0(1)*.

Migration

No changes.

CHAPTER 3

New features

- AS-SIP Line Endpoints, page 8
- Avatar device type, page 14
- Binary Floor Control Protocol, Real-Time Transport Control Protocol, and Far End Camera Control, page 37
- Codec preferences, page 39
- Confirmed Answer and DVO VM detection, page 41
- CTI support for Native Call Queuing, page 44
- Enhanced E911 support, page 45
- Enhanced Location Call Admission Control, page 46
- Enterprise Licensing Manager, page 61
- Fixed Mobile Convergence (FMC) over SIP trunks without Smart Client, page 63
- G.Clear support for BRI interfaces, page 65
- Hunt Pilot connected number, page 66
- HuntList connected number CTI support, page 67
- HCS Anonymous Call Rejection ISC Trunks, page 68
- HCS supplementary services for VoLTE IMS mobile device, page 70
- IM and Presence service consolidated administration, page 74
- Multiple syslog destination, page 76
- Native Call Queueing on CUCM, page 77
- NextGen mobile clients with QoE, page 88
- Originally Called Party Name in Placed Call History, page 89
- Pause in speed dials, page 91
- Record Line Key, page 92
- Secure Adhoc Conference MCU Setup, page 103

- Secure Cross Cluster Extension Mobility, page 105
- Serviceability for locations CAC enhancements, page 108
- Session Trace enhancement, page 113
- SIP CLI handling change, page 116
- SIP Diversion Counter, page 118
- SIP normalization and transparency, page 120
- Single step IP and hostname changes in CUCM cluster, page 121
- SNMP and billing setup using syslog destination address, page 128
- URI dialing and Intercluster Lookup Service, page 128
- User Options page enhancements, page 148
- Video for SNR call, page 149
- Video over Wi-Fi, page 151
- XML Axis framework 2.0 update, page 152
- 2000 character LDAP filter size, page 153

AS-SIP Line Endpoints

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

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

Cisco Unified Communications Manager Administration considerations

Unified CM supports Cisco Unified IP Phones with SIP as well as RFC3261-compliant phones that are running SIP from third-party companies. See the procedure to set up AS-SIP line endpoints for the steps to use Unified CM to manually configure a third-party phone that is running SIP.

Configuration Differences for Phones That Are Running AS-SIP

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

Phone Running AS-SIP	Integrated with Centralized TFTP	Sends MAC Address	Downloads Softkey File	Downloads Dial Plan File	Supports Unified Communications Manager Failover and Fallback	Supports Reset and Restart
Cisco Unified IP Phone 8961, 9951, 9971	Yes	Yes	Yes	Yes	Yes	Yes
Third-party AS-SIP device	No	No	No	No	No	No

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

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

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

AS-SIP Conferencing

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

- Local mixing
- Conference factory

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

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

How Unified Communications Manager Identifies a Third-Party Phone

Because third-party phones that are running SIP do not send a MAC address, they must identify themselves by using username.

The REGISTER message includes the following header:

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

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

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

Third-Party Phones That Are Running AS-SIP

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

End User Configuration Settings

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

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

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

Mulitlevel Precedence and Preemption Authorization

MLPP configuration and operation is slightly different for Assured Services SIP (AS-SIP) endpoints than for other MLPP endpoint devices. AS-SIP endpoints deliver the precedence level to the Unified CM via the resource-priority header. Other MLPP endpoints use the dialed number pattern to indicate the precedence level.

All AS-SIP phones support MLPP and function in the same manner as other MLPP devices. However, AS-SIP phone configuration is different since they do not rely on translations and routing functions within the Unified CM to establish the precedence level based on dialed digits. The AS-SIP device sends an explicit precedence level using a standard SIP resource-priority header. The collection of precedence information from the user by the endpoint is device-specific. Cisco AS-SIP phones provide a menu to allow the user to select a precedence level when making a call. This is also typical of third-pary AS-SIP endpoints, but may vary with different vendors. Regardless of phone type, the precedence level is signaled to the Unified CM in the same manner with no need for prepended digits to the called party. In addition, AS-SIP devices use an explicit SIP challenge method for MLPP authorization. This eliminates the need to use translation patterns and calling search spaces within Unified CM to control precedence authorization.

The explicit mechanisms for MLPP authorization and precedence establishment eliminate the need to configure the following items specifically for MLPP:

- Calling Search Spaces
- Translations/Routing Patterns

Note The configuration of these items may still be required for normal call operation, but not for MLPP.

Note For third-party endpoints, it is essential that the MLPP network domain, precedence domain, and precedence levels are configured in a manner consistent with the Unified CM configuration.

The following settings have been added to the End User Configurations Table:

Field	Description
MLPP User Identification Number	Enter a string of numeric characters. The MLPP User Identification number must be composed of 6 - 20 numeric characters.
MLPP Password	Enter a string of numeric characters. The MLPP Password must be composed of 4 - 20 numeric characters.
Confirm MLPP Password	To confirm that you entered the MLPP Password correctly, re-enter the password in this field.
MLPP Precedence Authorization Level	Set the MLPP Precedence Authorization Level. The Precedence Authorization Level can be set to any standard precedence level from Routine to Executive Override. Calls of equal or lower precedence are authorized to be originated by the user.

SIP Profile Configuration Settings

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

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

Adding and Configuring Third Party Phones

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

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

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

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

RTMT considerations

No changes.

Security considerations

Enabling Digest Authentication for Third-Party Phones That Are Running SIP

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

DTMF Reception

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

Phone Security Profile Configuration

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

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

TLS

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

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

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

Serviceability considerations

No changes.

Procedures

Set up AS-SIP line endpoints

This procedure lists the tasks used to manually configure a third-party phone that is running SIP. Use Cisco Unified Communications Manager Administration to configure third party phones.

Procedure

Step 1 Gather the following information about the phone:

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

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

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

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

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

- Resource Priority Namespace
- MLPP User Authorization

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

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

Step 5 Configure the phone security profile.
To use digest authentication, you must configure a new phone security profile. If you use one of the standard, nonsecure SIP profiles that are provided for auto-registration, you cannot enable digest authentication. See topics related to phone security profile configuration and the *Cisco Unified Communications Manager Security Guide* for more information.

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

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

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

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

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

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

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

CLI changes

No changes.

Avatar device type

CTI remote device setup

In Unified CM Administration, use the **Device** > **Phone** menu path to configure CTI Remote Device. CTI Remote devices configuration specifies a set of parameters that apply to all the CTI Remote Devices for the user.

CTI Remote Device type represents the users remote devices, similar to the Mobile Communicator device type. You can add a Remote Destination for a CTI Remote Device. The Remote Destination associated with the CTI Remote Device specifies the number to reach the Remote Device. The maximum number of Remote Destinations that you can configure for a CTI Remote Device is dependent on the Remote Destination limit set for the Owner User ID. By default, this value is set to 4.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

Additional information

CTI remote device setup tips

You can add a maximum of five Directory Numbers to the CTI Remote Device. To register a CTI Remote Device, add a Directory Number to that device. You cannot register a CTI Remote Device without a Directory Number.

Using the GUI

For instructions on how to use the Unified CM Administration GUI to find, delete, configure, or copy records, see topics that are related to the Unified CM Administration application in the *Cisco Unified Communications Manager Administration Guide*, which explain how to use the GUI and detail the functions of the buttons and icons.

CTI remote device configuration settings

The table below describes the available settings to configure a CTI remote device through the Phone Configuration Settings window.

Table 1: CTI remote device configuration settings

Field	Description
CTI Remote Device Information	
Device Information	
Registration	Specifies the registration status of the CTI Remote Device.
Device Status	Specifies if the device is active or inactive.
Device Trust	Specifies if the device is trusted.
Active Remote Destination	Specifies the Remote Destination which is active. The CTI client can specify one remote destination as 'active' at any one given time. Incoming calls and Dial via Office (DVO) calls are routed to the active remote destination.
Owner User ID	From the drop-down list box, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device.
Device Name	Specifies the name for the CTI Remote Device which is automatically populated based on the Owner User ID. The format of the device name is *CTIRD<OwnerUserID>* by default. You can also edit the device name. The device name can comprise up to 15 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the CTI remote device. This field can comprise up to 128 characters. You can use all characters except quotation marks (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Select the device pool that defines the common characteristics for CTI remote devices. For more information on how to configure the device pool, see “Device Pool Configuration Settings.”

Field	Description
Calling Search Space	Using the drop-down list box, choose the calling search space or leave the calling search space as the default of <None>.
User Hold MOH Audio Source	Using the drop-down list box, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Network Hold MOH Audio Source	Using the drop-down list box, choose the audio source to use for MOH when the network initiates a hold action.
Location	Using the drop-down list box, choose the location that is associated with the phones and gateways in the device pool.
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.
Call Routing Information	
Inbound/Outbound Calls Information	
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.
Protocol Specific Information	

Field	Description
Presence Group	Configure this field with the Presence feature. If you are not using this application user with presence, leave the default (None) setting for Presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.
Rerouting Calling Search Space	From the drop-down list box, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
Do Not Disturb Information	
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device.

Field	Description
DND Option	When you enable DND on the phone, Call Reject option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.

After you configure the CTI Remote Device, you can configure the associated remote destination. Click **Device** > **Phone** > **CTI Remote Device** > **Associated Remote Destinations** > **Add a New Remote Destination** to add and associate the remote destination with the CTI Remote Device.

Note You can configure a maximum of four unique Remote Destinations to associate with the CTI Remote Device.

When the Remote Destination is configured through the CTI Remote Device configuration window, the following parameters are altered.

- Mobile Phone—This function is disabled by default. The field cannot be edited and is not visible on the Administrative Interface.
- Enable Mobile Connect—This function is enabled by default. The field cannot be edited and is not visible on the Administrative Interface.

You can also configure the remote destination from **Device** > **Remote Destination** window. For more information about configuring remote destination, see Remote destination setup.

Note You cannot edit these two fields while you configure the Remote Destination through the CTI Remote Device Configuration window.

You can view the directory numbers that are assigned to the phone from the Association Information area of the Phone Configuration window. After you add a phone, the Association Information area displays on the left side of the Phone Configuration window.

Table 2: Association information settings

Field	Description
Modify Button Items	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this button to manage button associations for this phone. A dialog box warns that any unsaved changes to the phone may be lost. If you have saved any changes that you made to the phone, click OK to continue. The Reorder Phone Button Configuration window displays for this phone. See the "Modifying Phone Button Template Button Items" topic for a detailed procedure.
Line [1] - Add a new DN Line [2] - Add a new DN	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click these links to add directory numbers that associate with this phone. When you click one of the links, the Directory Number Configuration window displays. See the "Directory Number Configuration Settings" section for details.

CSF settings information

Cisco Client Services Framework setup

In Cisco Unified Communications Manager Administration, use the **Device** > **Phone** menu path to configure the Cisco Unified Client Services Framework device.

Note This section describes how to configure a Cisco Unified Client Services Framework device through the Phone Configuration Settings window.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

Additional information

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see topics related to Cisco Unified Communications Manager Administration application in the *Cisco Unified Communications Manager Administration Guide*, which explain how to use the GUI and detail the functions of the buttons and icons.

Client Services Framework configuration settings

The following table describes the available settings to configure a CTI remote device through the Phone Configuration Settings window.

Table 3: Client Services Framework Configuration Settings

Field	Description
Cisco Unified Client Services Framework Information	
Device Protocol	Specifies the protocol used to the Cisco Unified Client Services Framework.
Active Remote Destination	Specifies the Remote Destination which is active. The CSF client can specific one remote destination as 'active' at any one given time. Incoming calls and Dial via Office (DVO) calls are routed to the active remote destination.
Device Information	
Device Status	Specifies if the device is active or inactive.
Device Trust	Specifies if the device is trusted or not.

Field	Description
Device Name	Enter a text name for the Client Services Framework. This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description	Enter a text description of the Client Services Framework. This field can comprise up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Select the device pool which defines the common characteristics for Client Services Framework. For more information on how to configure the device pool, see Device Pool Configuration Settings.
Common Device Configuration	Using the drop-down list box, choose the common device configuration to which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window.
Phone Button Template	Using the drop-down list box, choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Common Phone Profile	Using the drop-down list box, choose the common phone profile to specify the data that is required by the Cisco TFTP.
Calling Search Space	Choose the calling search space to be used for routing Mobile Voice Access or Enterprise Feature Access calls. **Note** This calling search space setting applies only when you are routing calls from the remote destination, which specifies the outbound call leg to the dialed number for Mobile Voice Access and Enterprise Feature Access calls.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.

Field	Description
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If you choose <none>, Cisco Unified Communications Manager uses the Media Resource Group that is defined in the device pool.
User Hold MOH Audio Source	Using the drop-down list box, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Network Hold MOH Audio Source	Using the drop-down list box, choose the audio source to use for MOH when the network initiates a hold action.
Location	Using the drop-down list box, choose the location that is associated with the phones and gateways in the device pool.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
User Locale	From the drop-down list box, choose the locale that is associated with the CTI route point. The user locale identifies a set of detailed information to support users, including language and font. Cisco Unified Communications Manager makes this field available only for CTI route points that support localization. **Note** If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool. **Note** If the users require that information be displayed (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. See the Cisco Unified Communications Manager locale installer that is in the Cisco Unified Communications Operating System Administration Guide.

Field	Description
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. **Note** Choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
Device Mobility Mode	From the drop-down list box, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device. Click **View Current Device Mobility Settings** to display the current values of these device mobility parameters: • Cisco Unified Communications Manager Group • Roaming Device Pool • Location • Region • Network Locale • AAR Group • AAR Calling Search Space • Device Calling Search Space • Media Resource Group List • SRST For more configuration information, see "Device Mobility" in the *Cisco Unified Communications Manager Features and Services Guide*.
Owner User ID	From the drop-down list box, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.

Field	Description
Mobility User ID	From the drop-down list box, choose the user ID of the person to whom this dual-mode phone is assigned. **Note** The Mobility User ID configuration gets used for the Mobile Connect and Mobile Voice Access features for dual-mode phones. **Note** The Owner User ID and Mobility User ID can differ.
Primary Phone	Choose the physical phone that will be associated with the application, such as IP communicator or Cisco Unified Personal Communicator. When you choose a primary phone, the application consumes fewer device license units and is considered an "adjunct" license (to the primary phone). See "Licensing" in the Cisco Unified Communications Manager Features and Services Guide.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the "TRP Insertion in *Cisco Unified Communications Manager" in the Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the "Trusted Relay Point" section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Field	Description
Always Use Prime Line	From the drop-down list box, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco Call Manager service.
Always Use Prime Line for Voice Message	From the drop-down list box, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified CM always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Cisco Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco Call Manager service.
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Geolocation	From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System > Geolocation** Configuration menu option.

Field	Description
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls. Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call.
Allow Control of Device from CTIAllow Control of Device from CTI	Check this check box to allow CTI to control and monitor this device. If the associated directory number specifies a shared line, the check box should be enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Logged Into Hunt Group	This check box, which gets checked by default for all phones, indicates that the phone is currently logged in to a hunt list (group). When the phone gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.

Field	Description
Remote Device	If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device check box in the Phone Configuration window. Checking this check box tells Cisco Unified CM to allocate a buffer for the phone device when it registers and to bundle SCCP messages to the phone. **Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays for phones that are running SCCP. Most users do not require this option. Cisco Unified CM sends the bundled messages to the phone when the station buffer is full, as soon as it receives a media-related message, or when the Bundle Outbound SCCP Messages timer expires. To specify a setting other than the default setting (100 msec) for the Bundle Outbound SCCP Messages timer, configure a new value in the Service Parameters Configuration window for the Cisco CallManager service. Although 100 msec specifies the recommended setting, you may enter 15 msec to 500 msec. The phone must support SCCP version 9 to use this option. The following phones do not support SCCP message optimization: Cisco Unified IP Phone 7935/7936. This feature may require a phone reset after update.
Require off-premise location	
Call Routing Information	
Inbound/Outbound Calls Information	
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.
Protocol Specific Information	

Field	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. For more information on packet capturing, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. For more information on packet capturing, see the *Cisco Unified Communications Manager Troubleshooting Guide*.
Presence Group	Configure this field with the Presence feature. **Note** If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor.

Field	Description
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7905, 7912, 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to **<None>** if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.
MTP Preferred Originating Codec	From the drop-down list box, choose the codec to use if a media termination point is required for SIP calls.
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration. Installing Cisco Unified Communications Manager provides a set of predefined, nonsecure security profiles for auto-registration. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a nonsecure profile. To identify the settings that the profile contains, choose **System > Security Profile > Phone Security Profile**. **Note** The CAPF settings that are configured in the profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacturer-installed certificates (MICs) or locally significant certificates (LSC). See the Cisco Unified Communications Manager Security Guide for more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings.
Rerouting Calling Search Space	From the drop-down list box, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. For more information on digest authentication, see the *Cisco Unified Communications Manager Security Guide*.
Media Termination Point Required	Use this field to indicate whether a media termination point is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features. Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
Unattended Port	Check this check box to indicate an unattended port on this device.

Field	Description
Require DTMF Reception	For phones that are running SIP and SCCP, check this check box to require DTMF reception for this phone. **Note** In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation	From the drop-down list box, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone. For more information on CAPF operations, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options: • By Authentication String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC)—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC)—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.

Field	Description
Authentication String	If you chose the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.
Key Size (Bits)	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
Operation Completes By	This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation. The values that display apply for the publisher database server.
Certificate Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field.
Enable Extension Mobility	
Enable Extension Mobility	Check this check box if this phone supports extension mobility.
Log Out Profile	This drop-down list box specifies the device profile that the device uses when no one is logged in to the device by using Cisco Extension Mobility. You can choose either Use Current Device Settings or one of the specific configured profiles that are listed. If you select a specific configured profile, the system retains a mapping between the device and the login profile after the user logs out. If you select Use Current Device Settings, no mapping gets retained.

Field	Description
Log in Time	This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the user logged in displays in this field.
Log out Time	This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the system will log out the user displays in this field.
MLPP Information	
MLPP Domain	Choose an MLPP domain from the drop-down list box for the MLPP domain that is associated with this device. If you leave the None value, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
Do Not Disturb	
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device.
DND Option	When you enable DND on the phone, Ringer Off parameter turns off the ringer, but incoming call information gets presented to the device, so the user can accept the call.
Product Specific Configuration Layout Information	
Video Capabilities	When enabled, indicates that the device will participate in video calls. Default: Enabled

CLI changes

No changes.

Binary Floor Control Protocol, Real-Time Transport Control Protocol, and Far End Camera Control

Real-Time Transport Control Protocol pass-through in MTP topologies

An IOS Media Terminating Point (MTP) prior to 15.2(2)T, cannot pass-through Real-Time Transport Control Protocol (RTCP) packets. Therefore, an MTP cannot exchange Real-Time Protocol (RTP) feedback data to enhance the RTP transmission. The primary function of RTCP is to provide feedback of media distribution by periodically sending statistics to participants in a streaming multimedia session. RTCP gathers statistics for a media connection and information such as transmitted octet and packet counts, lost packet counts, jitter, and round-trip delay time. An application may use this information to control quality of service parameters, perhaps by limiting flow, or using a different codec.

IOS MTP Version 15.2(2)T and later supports RTCP pass-through capability so that the endpoint in a call with an MTP present can still provide feedback and status on an RTP transmission. RTCP pass-through capability applies on media channels.

The RTCP pass-through feature is not limited to a specific call signaling protocol. For example it can be SIP-SIP, SIP-nonSIP, or nonSIP-nonSIP.

In order for Cisco Unified CM to allocate an RTCP pass-through capable MTP specifically, the call must fulfill the following conditions:

- An MTP is requested for a feature that requires the MTP to be in media pass-through mode, for example, TRP, DTMF translation, or IP address V4/V6 translation. RTCP pass-through is only applicable when media are in pass-through mode
- The RTCP pass-through MTP must be included in the Media Resource Group Lists (MRGL) of the endpoint that sponsors the MTP. MTP can be inserted by RSVP, E2ERSVP, TRP, DTMF for reasons such as mismatch.
- When the call is capable of establishing video channels, Unified CM attempts to search for an RTCP pass-through-capable MTP. For example, Unified CM picks an RTCP pass-through-capable MTP from other noncapable ones in the MRGL. If an RTCP pass-through capable MTP is not available, Unified CM stills allocates an MTP for the call.
- When the call is capable of establishing an audio channel only, Unified CM does not request an RTCP-pass-through capable MTP for the non-video call. However, if the MRGL only contains RTCP-pass-through capable MTPs, Unified CM inserts one of those into the audio call.
- In order to have an RTCP pass-through capable MTP, the call also needs to fulfill the current Call Admission Control bandwidth for video call.

Note If a call initially establishes with a non-RTCP pass-through-capable MTP (prior to version 15.2(2)T) present in the call , and the call escalates into a video capable call, Unified CM does not reallocate to an RTCP-pass-through capable MTP. In that case, even though the call has been escalated to a video call, the existing MTP does not allow RTCP packets to be passed through.

Binary Floor Control Protocol Negotiation in MTP Topologies

A new version (15.2(2)T) of the IOS Media Terminating Point (MTP) router is now available which allows up to 16 media streams per session (previous release only allows up to three streams), this enables Cisco Unified Communications Manager to support Binary Floor Control Protocol (BFCP) and second video channels. A BFCP call normally requires at least four channels, audio, main video, second video and BFCP Control channel, to achieve video conferencing and also sharing presentations in the second video channel. If the call parties are capable of Far End Camera Control (FECC), a fifth channel would need to be established.

Note If the MTP does not have enough media ports to support a BFCP session, the BFCP media lines are not negotiated when the call is established.

Far End Camera Control

The Far End Camera Control (FECC) protocol allows you to control a remote camera. Within video calls, FECC allows the party at one end of the call to control the camera at the far end. This control can include panning the camera from one side to the other, tilting the camera, or zooming in and out. For video conferences that use multiple cameras, FECC can be used to switch from one camera to another.

Cisco Unified Communications Manager supports the FECC protocol for video endpoints that are FECC-capable. Cisco Unified Communications Manager supports FECC for SIP-SIP calls or H.323-H.323 calls, but does not support FECC for SIP-H.323 calls. To support FECC, Unified CM sets the application media channel through SIP or H.323 signaling. After the media channel is established, the individual endpoints can communicate the FECC signaling.

Note Prior to Unified CM Release 9.0, if an (MTP) was present in a SIP-SIP call, FECC was not available. For Unified CM Release 9.0, if there is an MTP (version 15.2(2)T or later) present in a SIP-SIP call, and there are five channels available for the call, then FECC can be enabled.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Codec preferences

The **System > Region Information > Audio Codec Preference** menu path is added to configure the order of audio codec preference, both for calls within a region and for between regions.

Cisco Unified Communications Manager Administration considerations

In Cisco Unified Communications Manager (Unified CM) Administration, use the **System > Region Information > Audio Codec Preference** menu path to configure the order of audio codec preference, both for calls within a region and for between regions.

Unified CM has two default Audio Codec Preference lists, one for lossy regions and another for low-loss regions. These are the Factory Default lossy, and the Factory Default low loss. Start with a default Audio Codec Preference list to create a custom list.

With the Audio Codec Preference feature, you can:

- Change the relative priorities of audio codecs.
- Save the custom Audio Codec Preference list with a unique name.
- Assign custom codec preference lists for use within a region or between regions.
- Create multiple custom codec preference list.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

Procedures

Create new Audio Codec Preference list

Procedure

Step 1 Click **Add New** from the **Find and List Audio Codec Preference lists** page.
The **Audio Codec Preference List Configuration** page is displayed.

Step 2 Choose an Audio Codec Preference list from the dropdown list.

Step 3 Click **Copy**.

Step 4 In the **Audio Codec Preference List Information** section, enter a Name and Description.

Step 5 Place the codecs in the preferred order by using the up and down arrows.

Step 6 Click **Save**.

Related Topics

Edit Audio Codec Preference list, on page 40
Delete Audio Codec Preference list, on page 41

Edit Audio Codec Preference list

Procedure

Step 1 In the **Audio Codec Preference** lists section, click the list to be edited.

The **Audio Codec Preference List Configuration** page is displayed.

Step 2 Reorder the audio codecs using the up and down arrows.

Step 3 Click **Save**.

Related Topics

Create new Audio Codec Preference list, on page 40
Delete Audio Codec Preference list, on page 41

Delete Audio Codec Preference list

Note You cannot delete the Factory Default lossy or low loss audio codec preference lists.

Procedure

Step 1 Select the list to be deleted from the **Audio Codec Preference lists** section.

Step 2 Click **Delete Selected**.
A message box appears "You are about to permanently delete one or more Audio Codec Preference Lists. This action cannot be undone. Continue?"

Step 3 Click **OK**.

Related Topics

Create new Audio Codec Preference list, on page 40
Edit Audio Codec Preference list, on page 40

CLI changes

No changes.

Confirmed Answer and DVO VM detection

Single Number Reach (SNR) Voicemail is a mobility enhancement to Unified CM that determines if users answer a call on their mobile devices from a remote destination (RD). By detecting if an RD call offered to mobile users reaches an external voicemail system, this feature provides users with a single enterprise voice mailbox for their enterprise mobility.

In order to prevent calls being answered by the mobile service provider voicemail, Unified CM implements a timer that determines whether or not the mobile service provider voicemail answers a call. This is required

to avoid situations where a mobile phone is switched off or unreachable. The network diverts immediately to mobile voicemail.

Note The single number reach voicemail feature is not supported for dusting calls.

Device Level Setting for RD/MI

For each RD and mobile identity (MI), there is a drop-down list box to configure the VoiceMail Selection Policy for supported devices. Acceptable values are Default, Timer Control, and User Control. The RD/MI page setting overrides the system wide setting. When you select Default, Unified CM defaults to the system setting via a service parameter.

Timer Control

Timer Control uses the Answer Too Soon timer to determine whether a call is answered by the mobile user or mobile service provider voicemail. If a call is answered within the Answer Too Soon Timer, SNR Voicemail determines that mobile service provider voicemail answered the call. As a result, this feature drops this call leg and reroutes the call to enterprise voicemail if no other shared line or remote destination answers the call.

User Control

When the user control is applied, Unified CM is ready to receive an explicit notification in the form of a DTMF digit, even after the voice channel connects a call.

Depending on the VoiceMail Selection User Control Delayed Announcement Timer, Unified CM may not insert any announcement. When you apply user control, Unified CM ensures that the PSTN side answers the call before extending the call.

If the client is not registered, the announcement always plays for RD or MI.

Note In case of a failure scenario, Unified CM tries to send an error message that indicates the call failure via data channel. For SendCallToMobile, Unified CM displays this error message on the desk phone with SendCallToMobile enabled: “Call fail due to Voicemail selection failure, please retry or contact system administrator.”

Cisco Unified Communications Manager Administration considerations

The following service parameters in Unified CM allow you to define the behavior of SNR Voicemail.

VoiceMail Selection Policy

The **VoiceMail Selection Policy** drop-down allows you to select either **Timer Control** or **User Control**. The default is set to **Timer Control**.

VoiceMail Selection User Control Delayed Announcement Timer

Unified CM uses this timer to delay the announcement that is played to RD users after they answer an RD call.

If Unified CM receives a user answer notification in DTMF or a data channel that the smartphone client generated, Unified CM does not play the announcement and connects the calling and called parties.

If Unified CM does not receive a user answer notification within the allotted time, Unified CM plays an announcement that prompts users to enter a DTMF digit to have their call connected.

If the client is able to send the DTMF digits or a notification via the data channel, the client ensures that the system sends the explicit answer notification after a user answers the call.

The default setting is 1 second.

VoiceMail Selection User Control Confirmed Answer Indication Timer

Cisco Unified Mobility uses this timer to wait for an answer notification, either from the received DTMF or from the mobile client via a data channel. When the timer expires, Cisco Unified Mobility drops the call.

The default setting is 5 seconds.

Note The Unified CM service parameter at the system level controls Single Number Reach Voicemail. The RD/MI device level setting controls the feature as well, however, the device level setting overrides the system setting. Unified CM uses the system setting if the device level setting is set to Default.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

CTI support for Native Call Queuing

For releases prior to Cisco Unified Communications Manager 9.0, it was very common in a Unified CM deployment that a hunt pilot had more calls distributed through the call distribution feature than its hunt members could handle at any given time. Native Queuing feature holds the calls in a queue until they are answered. When a hunt member is available, the call is removed from the queue and offered to the hunt member.

Complete documentation for this feature is provided in the Cisco Unified JTAPI Developers Guide.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Enhanced E911 support

Cisco Unified Communications Manager (Unified CM) can serve users on the customer premises and also users not on the customer premises (off-premises), using remote Virtual Private Network (VPN) connections. When users are on-premises, their location can be discovered automatically, by Unified CM Device Mobility or by Cisco Emergency Responder, for the purpose of determining how to route emergency calls to the appropriate Public Safety Answering Point (PSAP) and to indicate the caller's location to the PSAP. Without correct location information, emergency calls may reach a PSAP that is unable to dispatch emergency services to the caller's location, or emergency services may be dispatched to the wrong location.

The Remote Worker Emergency Calling feature supported by Unified CM and Emergency Responder enables customers to extend reliable emergency calling support to remote workers, by requiring remote workers to confirm or update their location whenever their device registration is interrupted. Users of devices designated for off-premises (connected remotely to the customer network) use are first presented with a (customizable) disclaimer notice, which assures that users are aware of the need to provide correct location information. Then the off-premises location currently associated with the designated device is presented. Users may confirm their current location or select another previously stored location from their device display; if their location is new, then they are directed to the Emergency Responder Off-Premises User web page to create a new location.

Prior to completion of this process, the user's device may be restricted by the customer to calling a single configured destination. This assures that the user has acknowledged the disclaimer and provided their current location information before the user's device is enabled for normal use.

Intrado V9-1-1 service validates and stores the location the user provides, and emergency calls from off-premises users are forwarded by Emergency Responder and Unified CM to Intrado. Intrado routes emergency calls to the PSAP with jurisdiction for the caller's location and delivers the user-provided location information together with each call.

The Remote Worker Emergency Calling features requires that the off-premises user be equipped with a hardware IP phone or software client that supports this feature. The customer must deploy Emergency Responder as well as Unified CM, and must subscribe to Intrado V9-1-1 emergency call delivery service. Intrado V9-1-1 service is available only in the United States.

Cisco Unified Communications Manager Administration considerations

Users of devices designated for off-premises use are first presented with various messages, which assure that users are aware of the need to provide correct location information.

The E911 Messages page allows you to view and edit the messages that can be displayed on an off-premises device. The Find-List for these messages is different than the traditional Find-List. Instead of listing individual messages, the list is shown as message sets based on the language, for example English, American. Selecting a language takes you to the page where you can edit and save the messages.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

Procedures

Set up E911 Messages

Use the following procedure to select and edit E911 messages for off-premises devices using Unified CM.

Procedure

Step 1 Choose **System** > **E911 Messages**.

Step 2 Select the required language link of the E911 messages.
The **E911 Messages Configuration** page displays the Agreement, Disclaimer, and Error messages.

Step 3 Optionally, you can edit the E911 messages to be displayed on off-premises devices.

Step 4 Click **Save**.

CLI changes

No changes.

Enhanced Location Call Admission Control

The Enhanced Location Call Admission Control (CAC) feature improves the Location CAC mechanism to support complex network, multi-tier, multi-hop topology. This feature supports Location CAC within a cluster and among multiple clusters and allows end to end bandwidth deduction. This enhancement to the CAC feature creates a much more flexible and dynamic system for the management of bandwidth.

The enhanced CAC feature provides a new service, called Location Bandwidth Manager (LBM). The LBM service can be configured to run on every node or selected nodes of a Cisco Unified Communications Manager (Unified CM) server.

Cisco Unified Communications Manager Administration considerations

The following tables provide changes and additions to the **Location info** of the Unified CM Administration:

Table 4: Location settings

Field	Description
Location Information	
Name	Enter the name of the new location that you are creating. Three system locations are predefined: • Hub_None—The Hub_None location specifies unlimited audio bandwidth and unlimited video bandwidth. A device that associates with the Hub_None location allows an unlimited number of active calls to or from the device. By default, devices not assigned to other locations are assigned to Hub_None. **Note** The location that is configured in a device pool takes precedence over the location configured in the device when the location in the device is set to Hub_None. If the device location is set to any other user-defined location, standard rules apply and the device parameter takes priority. • Phantom—Phantom location specifies unlimited audio bandwidth, unlimited video bandwidth, and unlimited immersive video bandwidth. Specify this location to allow successful call admission control for calls across intercluster trunks that use the H.323 protocol or SIP trunks to certain destinations that support the earlier Location CAC feature. **Note** Both Hub_None and Phantom locations do allow configuration of the associated RSVP policy settings. • Shadow—Shadow is a system location created for intercluster Enhanced Location CAC. In order to pass location information across clusters, the SIP ICT must be assigned to the system location Shadow.
Links - Bandwidth Between This Location and Adjacent Locations	
Location	Select a location from the list.
Weight	Enter the relative priority of this link in forming the effective path between any pair of locations. The effective path has the least cumulative weight of all possible paths. Valid values are 0 to 100.

Field	Description
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kbps) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Choose between the following options: • Unlimited bandwidth—Click the Unlimited radio button. • Specified bandwidth—Specify a bandwidth by clicking the radio button next to the kb/s box and entering a specified bandwidth. Valid values are 1 to 2147483647. For purposes of location bandwidth calculations only, assume that each call stream consumes the following amount of bandwidth: • G.711 call uses 80 kbps. • G.722 call uses 80 kbps. • G.723 call uses 24 kbps. • G.728 call uses 16 kbps. • G.729 call uses 24 kbps. • GSM call uses 29 kbps. • Wideband call uses 272 kbps. **Note** To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed on this link.
Video Calls Information	
Video Bandwidth	Enter the maximum amount of video bandwidth (in kbps) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Choose among the following options: • None—The system does not allow video calls between this location and other locations. • Specified bandwidth—Specify a video bandwidth by clicking the radio button next to the kbps box and entering a specified video bandwidth. The default value specifies 384 kbps. • Unlimited bandwidth—Click the Unlimited radio button.
Immersive Video Information	

Field	Description
Immersive Video	Enter the maximum amount of immersive video bandwidth (in kbps) that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead. Choose among the following options: • None—The system does not allow immersive video calls between this location and other locations. Immersive video calls can, however, take place within this location. • Specified bandwidth—Specify an immersive video bandwidth by clicking the radio button next to the kb/s box and entering a specified immersive video bandwidth. The default value specifies 384 kbps. • Unlimited bandwidth—Click the Unlimited radio button.
Intra-location - Bandwidth for Devices within This Location	
Audio Calls Information	
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link within this location. For audio calls, the audio bandwidth includes overhead. Choose between the following options: • Unlimited bandwidth—Click the Unlimited radio button. • Specified bandwidth—Specify a bandwidth by clicking the radio button next to the kb/s box and entering a specified bandwidth. Valid values are 1 to 2147483647. For purposes of location bandwidth calculations only, assume that each call stream consumes the following amount of bandwidth: • G.711 call uses 80 kb/s. • G.722 call uses 80 kb/s. • G.723 call uses 24 kb/s. • G.728 call uses 16 kb/s. • G.729 call uses 24 kb/s. • GSM call uses 29 kb/s. • Wideband call uses 272 kb/s. To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed within this location.
Video Calls Information	

Field	Description
Video Bandwidth	Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Choose among the following options: • None—The system does not allow video calls between this location and other locations. • Specified bandwidth—Specify a video bandwidth by clicking the radio button next to the kb/s box and entering a specified video bandwidth. The default value specifies 384 kb/s. • Unlimited bandwidth—Click the Unlimited radio button.
Immersive Video Information	
Immersive Video	Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead. Choose among the following options: • None—The system does not allow immersive video calls between this location and other locations. Immersive video calls can, however, take place within this location. • Specified bandwidth—Specify an immersive video bandwidth by clicking the radio button next to the kb/s box and entering a specified immersive video bandwidth. The default value specifies 384 kb/s. • Unlimited bandwidth—Click the Unlimited radio button.
Locations RSVP Settings	
Location	This display-only field displays locations for which the inter-location RSVP setting has been changed from the system default RSVP policy.
RSVP Setting	This display-only field displays the RSVP policy setting between the selected location and the location that is listed in the Location column to the left.
Modify Settings to Other Locations	
Location	To change the RSVP policy setting between the current location and a location that displays in this pane, choose a location in this pane.

Field	Description
RSVP Setting	To choose an RSVP policy setting between the current location and the location that is chosen in the Location pane at left, choose an RSVP setting from the drop-down list box. Choose from the following available settings: • Use System Default—The RSVP policy for the location pair matches the clusterwide RSVP policy. See topics related to clusterwide default RSVP policy in the *Cisco Unified Communications Manager System Guide* for details. • No Reservation—No RSVP reservations can get made between any two locations. • Optional (Video Desired)—A call can proceed as a best-effort audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP Agent continues to attempt RSVP reservation and informs Cisco Unified Communications Manager if reservation succeeds. • Mandatory—Cisco Unified Communications Manager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well. • Mandatory (Video Desired)—A video call can proceed as an audio-only call if a reservation for the video stream cannot be reserved.

Table 5: Location Bandwidth Manager Group configuration

Field	Description
Location Bandwidth Manager Group Setting	
Name	Enter the name of the new Location Bandwidth Manager Group that you are creating.
Description	If desired enter a description for the Location Bandwidth Manager Group.
Location Bandwidth Manager Group Members	
Active Member	Select the active member from the list.
Standby Member	If desired select a standby LBM to be used when the active LBM is not reachable.

Table 6: Location Bandwidth Manager Hub Group configuration

Field	Description
Location Bandwidth Manager Hub Group Information	
Name	Enter the name of the new Location Bandwidth Manager Hub Group that you are creating.

Field	Description
Description	If desired enter a description for the Location Bandwidth Manager Hub Group.
Location Bandwidth Manager Hub Group Members	
Member	Add members to the list.
Location Bandwidth Manager Hub Group Usage Information	
LBM Services Currently Use this LBM Hub Group	Add members to this list to use this LBM Hub Group.
LBM Services Do Not Use this LBM Hub Group	Members of this list do not use this LBM Group

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

Additional information

Enhanced Location Call Admission Control feature

The following sections provide information on the Enhanced Location Call Admission Control feature.

Terminology for Enhanced Location Call Admission Control

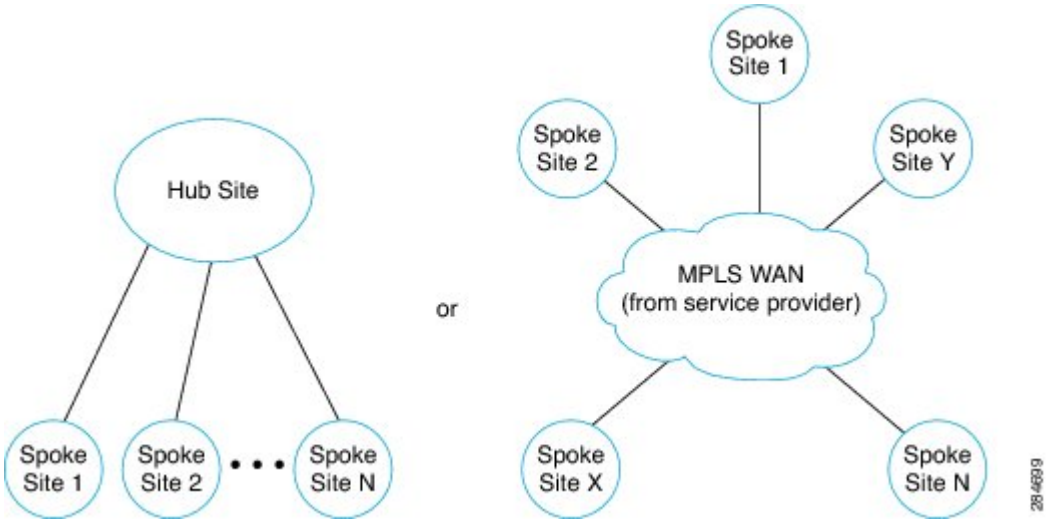
This document uses the following terms to discuss Enhanced Location Call Admission Control (CAC):

- **Link:** Links interconnect locations and are used to define the bandwidth available between locations.
- **Weight:**The relative priority of a link in forming the effective path between any pairs of locations. Weights are used on links to provide a "cost" to the "effective path". The effective path has the least cumulative weight of all other paths. Weights are pertinent only when there is more than 1 path between any 2 locations.
- **Locations:** A Location represents a LAN. It could contain endpoints or simply serve as a transit location between links for WAN network modeling
- **Bandwidth Allocation:** The amount of bandwidth allocated in the model for each type of traffic: audio, video, and immersive video (Telepresence).
- **Path:** A sequence of links and intermediate locations connecting a pair of end locations. Only one effective path between a pair of end locations is used
- **Locations Bandwidth Manager:** A service that assembles a network model from configured location and link data in one or more clusters, determines the effective paths between pairs of locations, determines whether to admit calls between a pair of locations based on the availability of bandwidth for each type of call, and deducts (reserves) bandwidth for the duration of each call that is admitted.
- **Locations Bandwidth Manager Hub:** An LBM service that has been designated to participate directly in inter-cluster replication of fixed and dynamic data. LBMs assigned an LBM hub group discover each other through their common connections and form a fully meshed replication network. Other LBM services in a cluster with an LBM hub participate indirectly in inter-cluster replication through the LBM hubs in their cluster.
- **Shadow location:** SIP Inter-cluster Trunks must be assigned to the Shadow location to enable proper inter-cluster operation of this feature. SIP trunks to devices with a specific location, such as SIP Gateways, may be assigned to ordinary locations. A Shadow location is a special location that has no links to other locations and no bandwidth allocations.

Limitations of bandwidth management prior to Release 9.0

Previously Unified CM Location Call Admission Control (CAC) could only effectively support the simple Hub and Spoke location model, such as remote sites connected to a main site or all sites connected to an MPLS-based IP WAN.

Figure 1: Hub and Spoke location model



Many customer networks do not conform to the Hub and Spoke location model; therefore customers need to have a Location CAC mechanism that better models the path that media actually travel through the network.

There are many deployments where multiple Unified CM clusters manage devices in the same physical site, for example, multiple Unified CM clusters manage phones in the same branch. When phones call each other within the same site but are managed by different clusters, bandwidth may be deducted (reserved) unnecessarily, which may cause blocking of other calls. Adding video calls and immersive video calls to the network exacerbates these issues because video calls consume more bandwidth than audio calls.

When Session Manager Edition (SME) attempts to manage bandwidth between clusters it can only assign location bandwidth to trunks connecting the SME and the leaf clusters, not reflecting the fact that media is may not be traversing the SME.

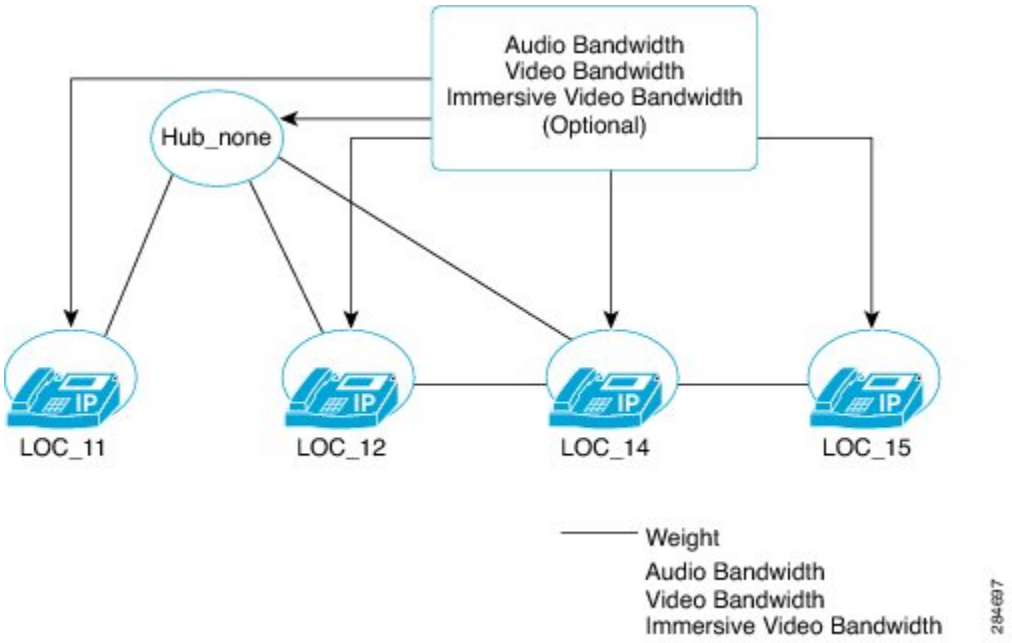
Enhancement to bandwidth management solution

The bandwidth management solution has been enhanced to support complex network models, including multi-tier, multi-hop topology. In these models audio and video calls can traverse multiple network links and locations and deduct bandwidth across each link. Enhanced network model is structured as follow:

- When two locations are directly connected, a link is modeled between them.
- Weights are assigned to the links to model the actual media path between two locations.
- Audio, video, and immersive video bandwidth capacity are assigned to each link and location.
- Bandwidth deductions are made from each link and from each location along the media path.

The following graphic represents a simple Location CAC topology model.

Figure 2: Simple Location CAC Model



Enhanced Location Call Admission Control architecture

The following sections provide information about Enhanced Location Call Admission Control architecture.

Model-based Call Admission Control

Enhanced Location Call Admission Control (CAC) is a model-based CAC mechanism. The administrator creates a model of the network and how the network infrastructure handles the media.

Note The more accurate and detailed the model of the network is, the more effective the management of the bandwidth and avoidance of congestion is within the network. However, the model cannot account for transient network failure conditions.

Through the Unified CM interface the administrator configures the Enhanced Location CAC mechanism based on the network model.

After the administrator creates the model and enters it into Unified CM database, Location Bandwidth Manager (LBM) calculates the effective paths between all originating and terminating locations, and deducts bandwidth from each link and location along that path.

When a call is admitted between two locations, LBM deducts (reserves) bandwidth from each link and location along that path for the duration of the call. The bandwidth deduction is symmetric (bidirectional). For example, for a G.711 audio call, 80 kb bandwidth is deducted from the audio allocation assigned to each link and location in the call path. When a call is terminated, LBM restores the bandwidth deduction.

The administrator may assign bandwidth allocations to locations as well as to links, if it is desired to limit admission of intra-location as well as inter-location calls.

Note The intra-location bandwidth allocations are unlimited by default.

Location Bandwidth Manager

A Location Bandwidth Manager (LBM) can reside and run on every Unified CM server, or on a few selected Unified CM servers within the cluster. LBM is a feature service and can be started and stopped from the serviceability configuration page.

Main functions of Location Bandwidth Manager are:

- Model Formation and path determination
- Replication of the model to other LBMs within the cluster, and between clusters
- Servicing bandwidth requests from Unified CM
- Replication of bandwidth deductions to other LBMs within the cluster, and between clusters
- Provide configured and dynamic information on request to Serviceability
- Update Location RTMT counters

When LBM service is started, it reads configured location information from the local database. This includes configured locations; audio, video, and immersive video capacities in those locations; links from a given location to other locations, the weight associated with those link; and the audio, video, and immersive video capacities on those links. It creates a local model with these values. Other LBMs in the cluster have access to the same data from the database and thus create the same local model at their startup. The LBM is now synchronized with the rest of the cluster and is ready to provide service.

Each Cisco Callmanager service communicates with LBM services within the cluster, as designated by an LBM group. By default, each Cisco Callmanager service communicates with the local LBM within the cluster.

Each LBM service communicates with all other LBMs within the cluster and may communicate through LBM Hubs with LBM services in other clusters. LBM services within the cluster are fully meshed.

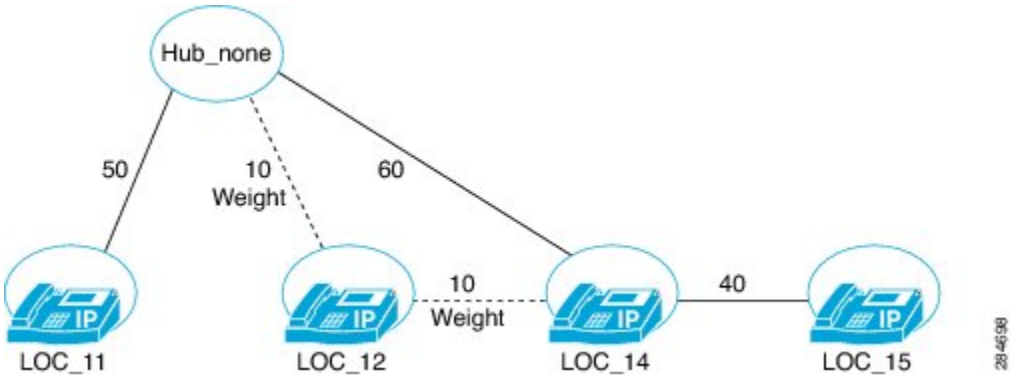
The LBM service computes the effective path from the source location to the destination location by adding the weight of each link for each possible path between source and destination. The path with the least cumulative weight is designated as the effective path. If there is more than one path that has the same weight LBM chooses which path to use. All calls that have the same source and destination locations use the same path.

The following figure provides an example, demonstrating the calculation of the effective path from Hub_none to Loc_14:

- A path from Hub_none through Loc_12 to Loc_14 is the effective path with a total weight of 20.

- A path from Hub_none to Loc_14 has weight of 60 which is greater than 20 and therefore not the effective path.

Figure 3: Location CAC effective reservation path determination



The following are some important considerations:

- LBM group configuration allows the administrator to select the LBM service that Unified CM can communicate with.
- It is not necessary to run the LBM service on every Unified CM server.
- The administrator can configure the LBM group based on consideration to minimize the network delay for bandwidth deduction.
- The LBM group can provide redundancy of LBM service to maintain the availability of CAC mechanism during network outage.
- When Unified CM is trying to locate the LBM service to communicate with:
  - It honors the LBM group association if one exists
  - If there is no LBM group assigned or an empty LBM group is assigned, Unified CM uses a local LBM if it is activated
  - If there is no LBM available, then Unified CM uses a service parameter to determine how to treat the call

When selectively activating LBM services and configuring the LBM groups consider the following: T

- Activate at least one LBM on each distinct call processing site. Consider activating LBM on standalone servers.
- For split data center deployment, activate at least one LBM for each data center.
- Consider activating LBM on the stand-by servers where there are active and stand-by servers to reduce the impact on the active servers.
- Connect to a local LBM service when available.
- For clusters with multiple sites, select LBM services in the data center or in the closest regional site.

Inter-cluster location Call Admission Control

With the model-based Location CAC between clusters (intercluster), each Unified CM cluster has a local model that it controls. Through an intersystem replication mechanism, each system in the enterprise network propagates its local model to other systems and creates a global model of the entire enterprise network by putting in each model from the remote systems, and storing it in the internal memory. LBM services in each system in the enterprise network that participate in the intercluster location CAC, has the global model stored in its local memory.

When a call is made across the clusters, originating and terminating systems pass their locations and call identifiers to each other through the signaling protocol (e.g. SIP signaling protocol). Terminating and originating clusters reserve location CAC bandwidth end to end locally, using its global location CAC model, and then replicate the bandwidth reservation to other systems in the enterprise network.

Note The amount of intersystem bandwidth replication messages can be significant. Select LBM Hubs carefully to make replication more efficient within the enterprise network.

Race conditions may occur as each local system reserves bandwidth from the global model and then replicates the deduction. When race conditions occur, calls may be admitted in excess of those for which bandwidth is deducted.

Note When modeling the network, use conservative bandwidth capacity assumptions to allow for the fact that calls may be admitted in excess of those for which bandwidth is deducted.

Intercluster location Call Admission Call configuration considerations

The following are some considerations when configuring intercluster location CAC between a local cluster and a remote cluster:

- The local administrator must configure the remote locations adjacent to local locations and the links between local and remote locations.
- When the local cluster receives a model replication from a remote cluster, it joins the models by identifying locations and links that appear in both models and forms a global network model.
- It is critical to name locations consistently in all clusters, to ensure the global network model assembles correctly. Follow the principle of same location, same name; different location, different name.

Note If there is a conflict in bandwidth capacity or weight assignment on the common links or locations, the local cluster uses the minimum of the assigned values.

Intercluster location Call Admission Control replication

An Enhanced Location CAC LBM replication network is used to replicate the model topology, and bandwidth deduction across multiple clusters, and within the cluster. All LBM services are fully connected within the cluster and all LBM Hubs are fully connected between clusters. LBM services that are not LBM Hubs participate in intercluster replication only through the LBM Hubs in their cluster.

The LBM Hub Group provides the mechanism for an LBM Hub to find out how to communicate with other LBM Hubs in remote clusters. By this mechanism, the LBM Hub builds a fully meshed replication network with all other LBM Hubs.

Location Bandwidth Manager Hubs

The following describes Location Bandwidth Manager (LBM) Hubs:

- An LBM service becomes a Hub when an LBM Hub Group is assigned to it.
- If a cluster has multiple LBM Hubs, the LBM Hub with the lowest IP Address functions as the sender of messages to other remote clusters.
- The LBM Hub organizes its links to remote LBM Hubs by the ClusterId assigned to it.
- The LBM Hub that functions as the sender for messages, and picks the first LBM Hub of each cluster to send messages to.
- The LBM Hub that receives messages from the remote clusters, forwards the received messages to other LBM services within the cluster.

Location Bandwidth service parameters

Service parameters for Enhanced Location Call Admission Control

There are three new service parameters for Enhanced Location CAC:

- **Unified CM to LBM Periodic Reservation Refresh Timer:** This parameter specifies the time duration in minutes that Cisco Unified Communications Manager refreshes the active bandwidth reservations to the Cisco Location Bandwidth Manager.
- **Call Treatment When No LBM Available:** This parameter specifies whether Cisco Unified Communications Manager allows or rejects calls when there is no Cisco Location Bandwidth Manager available for location-based call admission control.
- **Locations Media Resource Audio Bit Rate Policy:** This parameter determines the bit rate value to deduct from the audio bandwidth pools within and between the locations of the parties for an audio-only call when a Media Resource such as a transcoder is inserted into the media path and for more complex scenarios.

Shadow system location

Shadow location

Shadow is a new system location created for intercluster Enhanced Location CAC. In order to pass location information across clusters, the SIP ICT needs to be assigned to the system location Shadow.

The system location Shadow:

- Is a valid location only for a SIP ICT. Devices other than SIP trunks assigned incorrectly to the Shadow location are treated as if assigned to the Hub_None location.
- Cannot have a link connecting to other user defined locations, so bandwidth cannot be deducted between the Shadow location and other user defined locations.

- Has no intra-location bandwidth capacities, so bandwidth cannot be deducted within the Shadow location.

Note SIP trunks, including ICTs, may be assigned to fixed locations, if their destination does not participate in intercluster Enhanced Location CAC.

Devices that support Enhanced Location Call Admission Control

Device support

Unified CM and LBM manage bandwidth for all types of end devices, including IP phones, gateways, and H.323 and SIP trunk destinations. However, inter-cluster Enhanced Locations CAC requires SIP ICTs assigned to the system location Shadow. All other types of devices are supported only when assigned to ordinary (fixed) Locations.

Unified CM and LBM do not manage bandwidth for media resources; calls are modeled and bandwidth reserved between the locations of end devices only. For cases in which media resources change the bandwidth requirement for a call, the customer has the option to change a global parameter setting that determines whether the minimum or maximum bandwidth is reserved.

Enhanced Call Admission Control limitations

Limitations

The model created by the system is not perfectly synchronized at all times; excess calls may be admitted due to race conditions. Use conservative bandwidth allocations in the model to allow for this possibility.

During network failure conditions, the bandwidth reservation path calculated by Unified CM may not accurately reflect network conditions. There is no satisfactory way to allow for this scenario in the model.

Procedures

Configure Enhanced Location Call Admission Control

The Enhanced Location Call Admission Control (CAC) feature improves the Location CAC mechanism to support complex network, multi-tier, multi-hop topology. This feature supports Location CAC within a cluster and among multiple clusters and allows end to end bandwidth deduction. This enhancement to the CAC feature creates a much more flexible and dynamic system for the management of bandwidth.

The enhanced CAC feature provides a new service, called Location Bandwidth Manager (LBM). The LBM service can be configured to run on every node or selected nodes of a Cisco Unified Communications Manager (Unified CM) server.

Perform the following steps to configure the Enhanced Location Call Admission Control feature:

Procedure

Step 1 Activate the LBM service.
If a server is upgraded from pre-9.0 release, the LBM service is activated on all servers where the Cisco Callmanager service is enabled. For a new system install, the LBM service must be manually activated on the desired nodes.

Step 2 Create an LBM group.
Each Unified CM server must communicate with an LBM. If LBM is not running on the same node, configure an LBM group and assign the LBM group to the Unified CM server.

Step 3 Model the network using locations and links.

Step 4 Add the locations for the system.
By default, when a new location is created, a link from the newly added location to the Hub_None is added as well, with unlimited audio bandwidth, 384 kbps video bandwidth and 384 kbps immersive video bandwidth. This can be adjusted to match the model and if needed the link to the Hub_None location can be deleted.

Step 5 Assign intra-location bandwidth to the location, if the default of unlimited bandwidth is not desired.

Step 6 Add links from one location to other locations (inter-location). And assign bandwidth allocations and weight to the links.
If you are enabling intercluster Enhanced Location CAC complete the following steps:

Step 7 Configure the LBM Hub Group page to allow the LBM servers acting as Hubs to find LBM servers in remote clusters and establish external communication with those clusters.
Any LBM servers that are assigned an LBM Hub Group establish communication with all other LBM servers assigned the same or an overlapping LBM Hub Group.

Step 8 Assign the SIP ICT that is used to route calls between clusters to the system location Shadow.

CLI changes

No changes.

Enterprise Licensing Manager

Enterprise License Manager provides simplified, enterprise-wide management of user-based licensing, including license fulfillment. Enterprise License Manager handles licensing fulfillment, supports allocation and reconciliation of licenses across supported products, and provides enterprise-level reporting of usage and entitlement.

For more information on Enterprise License Manager, refer to the *Enterprise License Manager User Guide*.

Cisco Unified Communications Manager Administration considerations

Enterprise License Manager supports the following products:

- Cisco Unified Communications Manager

- Cisco Unity Connection

Enterprise License Manager can run on a separate server or virtual machine or can co-reside on a product's server or virtual machine. In a co-resident configuration, Enterprise License Manager is installed as part of the installation of Unified CM, Unity Connection, or both, as well as Unified Communications Manager Business Edition 5000 and Unified Communications Manager Business Edition 6000. For a standalone configuration, Enterprise License Manager must be installed separately.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Browser support

Enterprise License Manager supports the following browsers:

- Internet Explorer 7, 8, and 9
- Firefox 3, 4, 5, 6, 7, 8, and 9
- Mozilla 3 and 4
- Google Chrome
- Safari

CLI changes

license management

license management change user

This command takes parameters interactively and changes the username or password of the administrator.

license management change user {**name**| **password**}

Syntax Description

Parameters	Description
name	Specifies the administrator username.
password	Specifies the administrator password.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Enterprise License Manager

license management list users

This command lists the administrative users.

license management list users

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Enterprise License Manager

Fixed Mobile Convergence (FMC) over SIP trunks without Smart Client

Unified CM 9.0 allows service providers to provide base PBX-extension features such as enterprise dialing, SNR, single VM, call move, and mid-call features via the trunk without a smart client on the mobile. Basic mobile features such as Single Number Reach, Deskphone pickup, Send Call to Mobile, Mobile Voice Access and Mid-call DTMF features are supported. Extension dialing is supported if it is implemented in the network and the network is integrated with Unified CM. These features can be provided by any type of trunk.

With previous versions of Unified CM, service providers used the Remote Destination feature to deliver network-based FMC including the enterprise dialing/dial via office (DVO) feature without a client. This version allows for a new device type called Carrier-Integrated Mobile to deliver network-based FMC via the trunk or gateway.

When configuring the new device type Carrier-Integrated Mobile, set the Owner User ID value to the mobile user identity. The mobile user identity does not appear on the configuration page. Only end users with mobility enabled will appear in the Owner User ID drop-down list box on the End User page. Only one line (DN) can be associated with an FMC device. Users should associate a mobile identity with the FMC. This can be done on the FMC device configuration page after the device has been added. For calls to be extended to the number of the mobile identity, users must enable Mobile Connect on the Mobile Identity page.

Unified CM can be configured in the Ring All Shared Lines service parameter so that the shared-line is rung when mobile DN is dialed.

Note The Reroute Remote Destination Calls to Enterprise Number feature must be enabled for Ring All Shared Lines to take effect. Reroute Remote Destination Calls to Enterprise Number is disabled by default.

IP Multimedia System (IMS) shared lines ring solely based on the value of the Ring All Shared Lines parameter. In previous versions of Unified CM, IMS shared lines rang based on the value of Reroute Remote Destination Calls to Enterprise Number.

You can also migrate from the Remote Destination feature used in previous versions to this new device type.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

G.Clear support for BRI interfaces

Enable G.Clear Codec support for MGCP BRI gateways and SIP trunks. When the administrator enables G.Clear Codec, echo cancellation and zero suppression for outbound calls gets disabled.

Cisco Unified Communications Manager Administration considerations

Enable G.Clear Codec support for MGCP BRI gateways and SIP trunks. When you enable G.Clear Codec, echo cancellation and zero suppression for outbound calls are disabled.

Note Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager Administration do not work.

To enable G.Clear Codec support on SIP trunks between clusters, you must configure the SIP Clear Channel Data Route Class Label and SIP Route Class Naming Authority service parameters.

If you have low-bandwidth codec regions, you must enable the G.Clear Bandwidth Override service parameter.

The following functionality does not support the G.Clear Codec:

- T1 and E1 CAS
- H.323 Intercluster Trunks
- SCCP devices
- RSVP
- Frame aligning individual DS-0 circuits

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Hunt Pilot connected number

In Cisco Unified Communications Manager 9.0, the support for hunt pilots is enhanced to expose the hunt member which has answered the call as the called party in a call involving a hunt pilot at the calling side. With this enhancement, when a user calls a hunt pilot HP and the call is answered by the hunt list Line group member LG1, TAPI exposes DN of the HuntMember as the ModifiedConnectedParty DN under dev-specific part of linecallinfo under Call Party Normalization info structure. When this feature is disabled, the modifiedconnectedParty exposed is the HuntPilotDN. The Hunt Pilot Information is available in the dev-specific part of linecallinfo (under HuntPilotInfo structure). There is no change in Huntpilot information for call scenarios involving hunt pilot, when this feature is enabled from the information exposed when this is feature is disabled.

Cisco Unified Communications Manager Administration considerations

Enable **Display Line Group Member DN as Connected Party** to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

HuntList connected number CTI support

In Cisco Unified Communication Manager 9.0, the support for hunt pilots is enhanced to expose the connected number as the modifiedCalledAddress in a call involving a hunt pilot. With this enhancement, when a user calls a hunt pilot and the call is answered by the hunt member L1, call.getModifiedAddress() returns the address of the member L1, whereas call.getCurrentCalledAddress() returns the address of hunt pilot. Before the call is answered, both these values will return the address of hunt pilot.

Complete documentation for this feature is provided in the Cisco Unified JTAPI Developers Guide.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

HCS Anonymous Call Rejection ISC Trunks

Unified CM 9.0 allows the administrator to block incoming calls from anonymous callers. The administrator can choose to block these calls either at the SIP trunk or at the line or DN levels. Calls that originate from IP phones within the cluster or over other protocols with Calling Line ID Restriction (CLIR) will also get blocked.

There are three configuration options for the anonymous call rejection feature in Unified CM: one on the Directory Number page and two on the SIP Profile page.

Directory Number Configuration

To block outgoing anonymous calls for a particular line or DN, this feature can be configured on the Directory Number configuration page for the specific DN. Check the **Reject Anonymous Calls** check box on the Directory Number page to reject all anonymous calls for the DN.

In the case of an enterprise DN that has anonymous call rejection enabled and also has one or more single number reach destinations associated with it, Unified CM will block a call from anonymous callers to the enterprise DN and any of the remote destinations.

In the case of an enterprise DN that has anonymous call rejection enabled and also has a Call Forward All destination, Unified CM will forward anonymous calls to the CFALL target.

In the case of an enterprise DN that has anonymous call rejections enabled and also has a call forward on busy destination, Unified CM will reject the anonymous call without triggering call forward on busy.

The Call Forward No Answer feature is not triggered for an anonymous caller.

For Call Transfer - During attended transfer, if the transfer error has CLIR and places a consult call to a transfer-target who has ACR, the consult call will be rejected. Similarly on getting a REFER from anonymous caller, if the Refer-To DN has ACR, the REFER operation will be blocked. In both cases, the consult call will be blocked when the caller has CLIR and called party has ACR.

SIP Trunk Configuration

Configure anonymous call rejection on Unified CM to block calls from anonymous callers at the SIP trunk using the SIP Profile page configuration settings. Check the **Reject Anonymous Incoming Calls** and **Reject Anonymous Outgoing Calls** check boxes on the SIP Profile page. When the **Reject Anonymous Incoming Calls** check box is selected, all anonymous incoming calls on the SIP trunk associated this SIP Profile will be rejected. When the **Reject Anonymous Outgoing Calls** chec kbox is selected, all anonymous outgoing calls on the SIP trunk associated this SIP Profile will be rejected.

Anonymous calls in SIP are identified based on the criteria described in RFC 5079. Based on RFC 5079, calls are identified as anonymous when the incoming initial INVITE meets any of the following criteria:

- From or PAI/PPI header with display-name Anonymous
- From header host-portion = anonymous.invalid
- Privacy: id or Privacy: user or Privacy: header [associated with PAI/PPI]

- Remote-Party-ID header has a display-name Anonymous
- Remote-Party-ID header has privacy=uri/full

Note For calls that originate from within the Unified CM cluster, if the caller's DN or user information is present but caller name is not available or the presentation is restricted, the call is not marked as an anonymous call.

If the caller's DN is not present or the presentation is restricted, regardless of whether the caller's name is presented, the caller is deemed to be anonymous.

When Unified CM rejects an anonymous call, it sends SIP error response 433 - Anonymity Disallowed to the initial INVITE. Unified CM will also include Q.850 Reason header with cause = 21 (Call Rejected) in 433 response.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

HCS supplementary services for VoLTE IMS mobile device

Unified CM 9.0 supports a native way of invoking the supplementary services. The following supplementary services are supported:

- Originating Identification Presentation
- Terminating Identification Presentation
- Originating Identification Restriction
- Terminating Identification Restriction
- Communication Diversion Unconditional
- Communication Diversion on Not Logged in
- Communication Diversion on Busy
- Communication Diversion on Not Reachable
- Communication Diversion on No Reply
- Barring of All Incoming Calls
- Barring of All Outgoing Calls
- Barring of All Incoming Calls When Roaming
- Barring of Outgoing International Calls
- Communication Hold
- Communication Retrieve
- Third-Party Registration
- Message Waiting Indication
- Communication Waiting
- Ad Hoc Multiparty Conference
- Call Transfer

Originating Identification Presentation

The service control in the originating part is done by the home S-CSCF of the originator of the request. The originating S-CSCF can invoke services on behalf of the requestor.

When the initial inbound INVITE to an Intelligent Session Control (ISC) trunk has mode set to originating, Unified CM acts as the application server for the originating DN. In this scenario, Unified CM uses the user portion of the P-Asserted-Id to find the corresponding IMS client. When no such IMS client is found, Unified

CM rejects the call with a 403 forbidden error. After finding the corresponding IMS client, the call is routed through the enterprise DN configured for the IMS client.

The calling search space used for this call can either be a combination of line and IMS client's search space or the ISC trunk's, depending on the configuration of the IMS client.

Unified CM validates the destination through its DA . If the destination is not routable in the cluster, Unified CM will reject the call. Unified CM will not alert the destination and will not provide any terminating feature. After it is determined that the destination is routable, the call is anchored in Unified CM and then immediately routed out through the same ISC trunk, bypassing the RouteList or regular SIP trunk.

Note For unknown destinations to allow the IMS network to route to the default network, the Unified CM dial plan can have a default route through the ISC trunk for otherwise unknown destinations.

The originating call from the ISC trunk should not invoke Intelligent Session Control. If the mode is originating, CallControl does not send intercept to Intelligent Session Control even if the caller is the IMS client.

Terminating Identification Presentation

The service control in the terminating part is done by the home S-CSCF of the recipient of the request. The terminating S-CSCF can invoke services on behalf of the recipient.

When the initial inbound INVITE to an ISC trunk has the mode set to terminating, Unified CM acts as the application server for the terminating DN. In this scenario, Unified CM uses the user portion of the RequestURI to find the corresponding IMS client. When the IMS client is found, Unified CM treats the caller as an internal caller. This affects other feature interactions, such as Forwarding on Busy, Transfer to an external destination, and ad hoc terminating.

Unlike when serving as the originating side, Unified CM does not reject the call, even if the caller's P-Asserted-Id does not match any IMS client. Instead, it is treated as an external trunk call.

When acting as the application server for terminating DN, Unified CM alerts the destination and provides all terminating features.

If the destination includes an IMS client, the outbound INVITE goes through the same ISC trunk logically, but could be on a different node.

Note The terminating call invokes Intelligent Session Control. It is triggered by intercept by CallControl.

Call Forward

Unified CM 9.0 supports call forward treatments for the IMS client either through configuration or after a CFA activation request is received over the ISC trunk. The supported forwarding options are:

- CFA
- CF Not Logged In
- CFB
- CF Not Reachable
- CFNA

Call Barring

Unified CM 9.0 provides call barring functionality. This feature allows you to block calls in the following ways:

- Barring of All Incoming Calls
- Barring of All Outgoing Calls
- Barring of All Incoming Calls When Roaming
- Barring of Outgoing International Calls

A new section was added to the Phone Configuration page for Call Barring Information. In this section you can check the check box to **Block Incoming Call while Roaming** and define the **Home Network ID**.

Note The **Home Network ID** must be defined to enable the **Block Incoming Call while Roaming** feature.

Hold

Unified CM supports hold feature invocation through Invite coming in from the ISC interface. Upon receiving the Invite, Unified CM places the active call on hold and allocates the necessary Music On Hold resource to stream to the held party, if configured. The IMS network-triggered hold receives the same treatment as the internal user-originated hold operation.

Retrieve

Unified CM now supports Retrieve requests over the ISC interface on a held call in the form of Invite with SendReceive SDP. Upon receiving such request, Unified CM will apply its Retrieve call operations, such as remove and de-allocate any Music On Hold resources, and reconnect the media between two parties.

Third-Party Registration

Unified CM 9.0 provides a third-party registration feature.

A new check box for **Third-party Registration Required** was added to the Protocol Specific Information section.

Message Waiting Indication

Unified CM 9.0 supports subscription from the IMS client in the IMS core network through the SUBSCRIBE method. Upon receiving the SUBSCRIBE request from the IMS core, Unified CM determines if the requesting client is qualified to receive Message Waiting Indication (MWI) notification by checking the client provisioning data. If the client is qualified, Unified CM delivers the cached MWI data to the client upon completing the SUBSCRIBE handling, and continues to deliver the MWI notification if there is any MWI status change under the condition that the subscription is still valid.

Call Waiting

Unified CM 9.0 allows the user to select from various call waiting options. If a mobile user has an active call and a new incoming call arrives, the user has the options to:

- Ignore the new incoming call.

When the user selects this option, the call forwarding treatment may be applied if the forward on busy configuration is set.

- Quit the incoming call.

  When the user selects this option, the call forwarding treatment may be applied if the forward on no answer configuration is set.

- Answer the incoming call.

  When the user selects this option, the original active call is put on hold first, and then the new call can be answered.

IMS Client-Initiated Ad Hoc Conference Request

The single user conference begins with an Invite with a specified conference service request URI. Upon receiving such a service request URI, the conference feature dynamically allocates a number as the conference identifier and registers that number with the Unified CM internal DA service. The conference feature allocates the conference resource and creates the conference for the user that initiated the conference service request. The dynamically allocated conference identifier number is used to identify the existing conference and allow a new participant to be added to the same conference.

The conference service request URI must be provisioned through a new service parameter within Unified Communications Manager to ensure the correct behavior of the single user conference creation procedure. This provisioning of service parameter must match what is provisioned in the IMS core network. For instance, the URI can be configured as cucm-conference-factory@cucm1.company.com.

Additional conference participants will ride with a Refer with the existing dialog for all calls respectively. The call information in this Refer has the conference ID that the conference feature allocated during the single user conference creation. The Unified CM Refer/Replace feature picks up the task and joins the participant to the existing single user conference. The Refer feature applies the same mechanism to add all of the conference participants.

Note The new conference flows for single user conference creation and the ability to add and drop conference participants are available only when the request is sent from a Unified CM provisioned IMS client on the IMS core network. If this is not the case, the request will be rejected.

Transfer

Unified CM can handle transfer requests from the IMS core network. The transfer is done through SIP Refer/Replace method in the ISC interface.

Note Calls are put on hold before the transfer is initiated from the IMS client.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

IM and Presence service consolidated administration

In Unified CM, administrators can set up end users for IM and Presence, add unified communications (UC) services, service profiles, and associate service profiles to end users from a consolidated administration interface.

Cisco Unified Communications Manager Administration considerations

The User Management menu contains the following updates:

- **User Management** > **End User** contains a new section called Service Settings. This section contains three new fields: Home Cluster, Enable User for Unified CM IM and Presence, and UC Service Profile. These fields allow administrators to home an end user to a cluster (required for IM and Presence), enable the end user for IM and Presence, and assign a UC Service Profile that they create in the following menu item.
- **User Management** > **User Settings** > **UC Service** is a new Unified CM menu item that allows administrators to set up the following UC services for clients:
    - Voicemail
    - Mailstore
    - Conferencing
    - Directory
    - IM and Presence
    - CTI

After administrators add these services to the Unified CM database, they can group them into a service profile in the following menu item. After end users have a service profile, their clients can download this profile for seamless integration with the configured UC services.

- **User Management** > **User Settings** > **Service Profile** is a new Unified CM menu item that allows administrators to group UC services into service profiles. Administrators specify primary, secondary, and tertiary servers. After administrators save a service profile, they can associate it to an end user, and end user clients can download this profile for seamless integration with the configured UC services.
- **User Management** > **User Settings** > **Quick User/Phone Add** > **Universal Device Templates** is a new Unified CM menu item that allows administrators to create templates that are model-independent and apply them to devices that they add to the Unified CM database.
- **User Management** > **User Settings** > **Quick User/Phone Add** > **Universal Device Template Page Layout Preference** is a new Unified CM menu item that allows administrators to customize the order of sections for the **Universal Device Templates** window, in order to simplify the window view and list sections that are relevant to the administrator tasks.
- **User Management** > **User Settings** > **Quick User/Phone Add** > **Feature Group Templates** is a new Unified CM menu item that allows administrators to create feature group templates to apply to users. Like the **End User** window, the **Feature Group Templates** window contains fields to set up a user for IM and Presence. On this window, administrators universal device templates for desk phones, mobile devices, and profiles, which they next associate to the user in the following window.
- **User Management** > **User Settings** > **Quick User/Phone Add** > **Quick User/Phone Add** is a new Unified CM menu item that gives administrators a simplified way to add users and phones to the Unified CM database. At this window, administrators set up basic user information, access control group membership, credentials, and so on. Here, administrators assign a feature group template to the user. They may also move an existing device in the system to this user.

Bulk Administration considerations

- **Bulk Administration** > **Users** > **User Template** contains three new fields under the section User Template Configuration: Home Cluster, Enable User for Unified CM IM and Presence, and UC Service Profile. These fields allow administrators to home an end user to a cluster (required for IM and Presence), enable the end user for IM and Presence, and assign a UC Service Profile as part of the user template.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Multiple syslog destination

This feature enables you to configure multiple remote syslog servers in Cisco syslog agent enterprise parameters.

Cisco Unified Communications Manager Administration considerations

The System menu contains the following updates:

- **System** > **Enterprise Parameters**—The following fields have been added:
  - Remote Syslog Server Name 1
  - Remote Syslog Server Name 2
  - Remote Syslog Server Name 3
  - Remote Syslog Server Name 4
  - Remote Syslog Server Name 5
- **System** > **Enterprise Parameters**—The Remote Syslog Server Name field has been removed.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

The Alarm menu contains the following updates:

- **Alarm** > **Configuration**—The following fields have been added:
  - Server Name 1
  - Server Name 2
  - Server Name 3
  - Server Name 4
  - Server Name 5

CLI changes

No changes.

Native Call Queueing on CUCM

Unified CM provides call queuing natively to users so that callers can be held in a queue until hunt members are available to answer them. Callers in a queue receive an initial greeting announcement followed by music on hold or tone on hold. If the caller remains in queue for a period of time, a secondary announcement is played at a configured interval until the call can be answered—or until the maximum wait timer expires.

Cisco Unified Communications Manager Administration considerations

The Call Queuing feature provides an enhanced capability to handle incoming calls to a hunt pilot number. When an incoming call reaches the hunt pilot, the following capabilities are provided:

- A caller may be connected to an initial customizable greeting announcement before proceeding
- If one or more line members are logged into the hunt pilot and are in an idle state, and if no calls are queued, then the call is extended to the line member that has been idle for the longest period of time
- If no line members answer a call, then that caller is placed in a holding queue
- If a line member does not answer a queue-enabled call, that line member is logged off automatically
- While the caller is in the queue they may hear Music On Hold and a repeating (customizable) periodic announcement
- Once a line member becomes idle, the caller with the longest wait time across multiple hunt groups is extended to the idle line member. If the idle line member does not answer the call, the caller is returned to their previous position in the queue
- If a queued call exceeds its maximum wait time, it can be routed to another pattern or it can be disconnected, depending upon how the hunt pilot configuration is configured
- If the maximum number of callers allowed in queue has been reached, any subsequent caller can be routed to another pattern or disconnected, depending upon how the hunt pilot configuration is configured
- Line members can display the queue status of their queue-enabled hunt pilots (in other words, the hunt pilots with which they are associated). The queue status display provides the following types of information:

- Hunt pilot pattern
- Number of queued callers on each hunt pilot
- Longest waiting time

For shared-line deployments, the availability of all devices with that shared-line are combined to provide a final status. If a shared-line device for one or members appears as on-hook, but all others are indicating off-hook, the final status for that line member remains on-hook.

Call queuing works in conjunction with existing hunt pilots, but there are no changes in the behavior of the hunting mechanism for either queuing or non-queuing hunt pilots. There are, however; specific features associated with hunt pilots that have call queuing enabled:

1. Queuing-enabled hunt pilot calls can only be received by line members one call at a time. Two queuing-enabled hunt pilot calls cannot be offered to a line member (no matter what the busy trigger is set to). This does not limit a line member to only receive calls directly to their DN or from non-queuing hunt pilots.
2. Line members who do not answer hunt pilot routed calls are automatically logged out. A line member is automatically logged out of a device if the line member receives a queuing-enabled hunt pilot call and does not answer the call until an RNA reversion time-out occurs. In the case of a shared-line deployment, all devices configured with the same shared-line are logged out.

While the calling party is in queue, the caller receives a MoH treatment depending upon the network MoH settings for that hunt pilot. There is option available to play the initial announcement first and then offer a call to a hunt pilot. If the call is not answered by any of the line members, the caller is placed on hold (in queue) with an announcement provided periodically in addition to MoH. The second option involves offering the call to a hunt pilot DN first, and then place caller on hold (in queue) if the call is not answered. Again, an announcement is provided periodically in addition to MoH. When a line member becomes available to answer the next caller in the queue, the call that has been in the queue the longest is offered to line member. If the line member does not answer the call, the caller is placed back in the queue at the same position.

Alternate Number Configuration

Call Queuing configuration provides for the routing of calls to an alternate number. These alternate numbers may be:

- A hunt pilot DN with queuing either enabled or disabled
- A voice mail DN
- A line DN
- A shared DN

There are three main scenarios where alternate numbers are used:

1. When queue is full
2. When maximum wait time is met
3. When no hunt members are logged in or registered

Call Queuing allows up to 100 callers to be queued per hunt pilot (the maximum number of callers allowed in queue on a hunt pilot page). Once this limit for new callers been reached on a particular hunt pilot, subsequent calls can be routed to an alternate number. This alternate number can be configured through the Hunt Pilot configuration page (through the “Destination When Queue is Full” settings).

Each caller can be queued for up to 3600 seconds per hunt pilot (the maximum wait time in queue). Once this limit is reached, that caller is routed to an alternate number. This alternate number can be configured through the Hunt Pilot configuration page (through the "Maximum wait time in queue" settings).

In a scenario where none of the members of the hunt pilot are available or registered at the time of the call, hunt pilot configuration provides an alternate number field (through the "When no hunt members are logged in or registered" settings) where calls can be routed. For Call Queuing, a hunt pilot member is considered available if that member has both deactivated do not disturb (DND) and logged into the hunt group. In all other cases, the line member is considered unavailable or logged off.

Music on Hold

MoH capabilities have been enhanced to play an optional initial greeting announcement when a caller is first put on hold and also to play a periodic repeating announcement when a caller is hearing the normal MoH audio. These announcements can use one of the Cisco-provided audio files or a custom file that is uploaded into the system.

Music on Hold Audio Source Configuration Settings

The following updates have been made to the Music on Hold Audio Source Configuration Settings Table for the Call Queuing feature:

Field	Description
MoH Audio Source	
(list of MoH audio sources)	For each MoH audio source that has been added, the MoH audio source name displays in this list box. Click the audio stream number of an MoH audio source to configure that MoH audio source. **Note** If <None> is selected, the system default MoH audio source service parameter (Default Network Hold MoH Audio Source ID) is used for the MoH audio source.
Announcement Settings	
Initial Announcement	Choose an initial announcement from the drop-down list box. **Note** To select MoH with no initial announcement, choose the default option: "Not Selected". Select View Details to view the following Initial Announcement information: • Announcement Identifier • Description • Default Announcement

Field	Description
Initial Announcement Played	Choose one of the following to determine when the initial announcement is played: • Always- for all calls (default) • Only for queued calls - in situations when no agents are available.
Periodic Announcement	Choose a periodic announcement from the drop-down list box. **Note** To select MoH with no periodic announcement, choose the default option: "Not Selected". Select View Details to view the following Periodic Announcement information: • Announcement Identifier • Description • Default Announcement
Periodic Announcement Interval	Enter a value (in seconds) that specifies the periodic announcement interval. Valid values specify 10 to 300. The default value is 30.
Locale Announcement	Locale Announcement depends upon the locale installation package that has been installed.

Announcement Configuration

Cisco-provided announcements and tones are installed automatically when you install Cisco Unified Communications Manager. These announcements and tones are displayed in the Find and Lists Announcements window in Cisco Unified Communications Manager Administration. Announcements can be used for:

- Basic calls
- External call control
- Multilevel Precedence and Preemption (MLPP)

Selecting **Media Resources > Announcements** in Cisco Unified Communications Manager allows you to use the existing Cisco-provided announcements, insert custom announcement .wav files, assign the locale for the announcement, change the description for the announcement, or change the message or tone that you wish an announcement to play.

Announcement Configuration Settings

In Cisco Unified Communications Manager Administration, use the **Media Resources > Announcements** menu path to configure announcements. There are two classifications of announcements:

- System Announcements

- Feature Announcements

System announcements are pre-defined announcements that are used in normal call processing or provided as sample feature announcements. Feature announcements are used by specific features such as Music On Hold (MoH) in association with Hunt Pilot call queuing or External Call Control.

There are up to 50 feature announcements available using the Add New button. These announcements may be Cisco-provided audio files or uploaded custom wav files. All custom announcement wav files must be uploaded to all servers in the cluster.

Note Announcements are specific to the locale (language). If your installation is using more than one language locale, each custom announcement must be recorded in each language as a separate wav file and uploaded with the correct locale assignment. This also requires that the correct locale package be installed on each server before uploading custom announcement wav files for languages other than United States English.

From the Announcement Listing window, clicking on the announcement identifier for an announcement produces an announcement configuration dialog. Within this dialog you can edit the announcement description and other settings. If one or more custom wav files have been uploaded for the announcement, a list of the custom wav files for each locale (language) is created. Each of these files also have an Enable check-box to indicate if the custom wav file should be used. If the check-box is unchecked, then the selected Cisco audio file is used. Like MoH audio source files, the recommended format for announcements includes the following specifications:

- 16-bit PCM wav file
- Stereo or mono
- Sample rates of 48 kHz, 44.1 kHz, 32 kHz, 16 kHz, or 8 kHz

Configuration Setting Table

The following updates have been made to the Configuration Settings Table for the Call Queuing feature:

Field	Description
Announcement Configuration and Upload File Windows	
Announcement Identifier	The Announcement Identifier is a text box to assign a meaningful identifying name to the announcement. This field cannot be modified for System Announcements. This field must be unique (different from all other announcements). The Announcement Identifier is used when selecting an announcement for a feature such as Music-on-Hold.

Field	Description
Customized Description	For customized announcements that you are inserting, enter a description for the announcement (for example, enter the text from the customized announcement). You can enter any characters in this field. When you click the Upload File button in the Find and List window, this field displays as blank. When you click the Upload File button in the Announcements Configuration window, the Cisco-provided (default) description for the announcement displays. If you do not update this field in the Announcements Configuration window, the Cisco-provided (default) description displays. After you update this customized description field, the Cisco-provided description displays in the Find and Lists Announcements window. See the Default Description column in the Find and Lists window for the default description. You can enter up to 50 characters.
Locale	This setting displays in the Upload File window. From the Locale drop-down list box, choose the locale that you want to associate with the announcement. By default, all Cisco-provided announcements support English_United States. If a Cisco Unified Communications Locale has been installed, the Cisco-provided announcements are provided for that locale in addition to other installed locales. **Tip:** For a locale to display in the Locale drop-down list box in the Upload File Configuration window, you must install the Cisco Unified Communications Locale Installer that is specific to your locale(s). For more information, see the Cisco Unified Communications Operating System Administration Guide.
Default Announcement	From the drop-down list box, choose the Cisco-provided announcement that you want to play when the custom announcement is not used. If <None> is selected from the list box, no Cisco-provided announcement will be used.
Announcement by Locale Pane in the Announcements Configuration Window **Note** This section only appears if a custom announcement wav file has been uploaded for the announcement.	

Field	Description
Enable	This setting displays after you insert a customized announcement. When the Enable check box is checked, Cisco Unified Communications Manager plays the customized announcement for the locale that is shown. If you want Cisco Unified Communications Manager to play the Cisco-provided announcement that is associated with the announcement identifier, uncheck the Enable check box.
Customized Locale Description	This field, which is read-only, displays the description for the customized announcement for the displayed locale. You enter this description when you upload the customized announcement.
Locale	This field, which is read-only, displays the locale that you chose for the customized announcement when you uploaded the .wav file. Each locale is associated with an uploaded custom announcement. You can upload another wav file for the same announcement, but you assign it to a different locale. In this case, two rows would display, one for each locale. If you want to update or replace a custom announcement for a locale, you can upload a new wav file with the same locale you want to replace.
Default Cisco Announcement	This field indicates the last uploaded customized announcement file name.

Hunt Pilot Configuration Settings

The following updates have been made to the Configuration Hunt Pilot Configuration Settings Table for the Call Queuing feature:

Field	Description
Pattern Definition	
Call Pickup Group	Choose the number that can be dialed to answer calls to this directory number (in the specified partition). **Note** The Call Pickup Group setting has been moved to this section from the Forward settings section.
Hunt Call Treatment Settings (Previously called Hunt Forward Settings)	

Field	Description
Forward Hunt No Answer	When the call that is distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose from the following options: • Do Not Forward Unanswered Calls • Use Forward Settings of Line Group Member (replaces "Use Personal Preferences" check box) • Forward Unanswered Calls to: – Destination—This setting indicates the directory number to which calls are forwarded. – Calling Search Space—This setting applies to all devices that are using this directory number. • Maximum Hunt Timer—Enter a value (in seconds) that specifies the maximum time for hunting without queuing. Valid values specify 1 to 3600. The default value specifies 1800 seconds (30 minutes). This timer cancels if either a hunt member answers the call or if the hunt list gets exhausted before the timer expires. If you do not specify a value for this timer, hunting continues until a hunt member answers or hunting exhausts. If neither event takes place, hunting continues for 30 minutes, after which the call gets taken for final treatment. **Note** If hunting exceeds the number of hops that the Forward Maximum Hop Count service parameter specifies, hunting expires before the 30-minute maximum hunt timer value, and the caller receives a reorder tone. In addition, Cisco Unified CM only uses the configuration for the Maximum Hunt Timer setting if you configure the Hunt Forward settings in the Hunt Pilot Configuration window.

Field	Description
Forward Hunt Busy	When the call that is distributed through the hunt list is busy in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose from the following options: • Do Not Forward Busy Calls • Use Forward Settings of Line Group Member • Forward Busy Calls to: ◦ Destination—This setting indicates the directory number to which calls are forwarded. ◦ Calling Search Space—This setting applies to all devices that are using this directory number.
Note Forward Hunt No Answer or Forward Hunt Busy settings are designed to move calls through the route list. Queuing, on the other hand, is used to hold callers in a route list. Therefore, if queuing is enabled, both Forward Hunt No Answer and Forward Hunt Busy are automatically disabled. Conversely, if Forward Hunt No Answer or Forward Hunt Busy are enabled, queuing is automatically disabled.	
Queue Calls	Check the Queue Calls check box to enable queuing. When a hunt pilot has more calls distributed through the call distribution feature than its hunt members can handle at any given time, call queuing holds these calls in a queue until they can be answered. Once Queue Calls has been selected, choose from the following options:

Field	Description
Network Hold/MoH Source and Announcements	Choose a Music On Hold (MoH) source from the drop-down list box, which will be used to play announcements and provide queue hold treatments. The default value is NULL. If nothing is selected, the default Network Hold MoH/MoH Source and Announcements configured on service parameter is used. The MoH source can be configured as unicast or multicast. Caller side's MRGL takes precedence for multicast or unicast. The MoH source announcement locale is used to determine the language used for the announcement. Only one type of language announcement can be played per hunt pilot. When any of the MoH settings are changed, the existing callers in queue are not affected. All future queued callers will listen to MoH and announcements as per the updated settings.
Maximum Number of Callers Allowed in Queue	Enter an integer value for the number of callers allowed in the queue for this hunt pilot. The default value is 32. The field range is from 1 to 100. When the maximum number of callers in queue has been reached, and if subsequent calls need to be disconnected, select the “Disconnect the call” radio button. When the maximum number of callers in queue has been reached, and if subsequent calls need to be routed to a secondary destination, select the “Route the call to this destination” radio button. Provide a specific device DN, shared line DN, or another Hunt Pilot DN. You may also select the “Full Queue Calling Search Space” from the drop-down list (optional).

Field	Description
Maximum Wait Time in Queue	Enter an integer value to set the maximum wait time, in seconds, in a queue. The default value is 900 seconds. The field range is from 10 to 3600 seconds. When the maximum wait time in queue has been reached, and if the queued caller needs to be disconnected, select the “Disconnect the call” radio button. When the maximum wait time in queue has been reached, and if the queued caller needs to be routed to a secondary destination, select the “Route the call to this destination” radio button. Provide a specific device DN, shared line DN, or another Hunt Pilot DN. You may also select the “Maximum Wait Time Calling Search Space” from the drop-down list (optional).
When no hunt members are logged in or registered	When no line members are logged in or registered at the time of an incoming call, and if that call needs to be disconnected, select the “Disconnect the call” radio button. When no line members are logged in or registered at the time of an incoming call, and if that call needs to be routed to a secondary destination, select the “Route the call to this destination” radio button. Provide a specific device DN, shared line DN, or another Hunt Pilot DN. You may also select the “No hunt members logged in or registered Calling Search Space” from the drop-down list (optional).
Calling Party Transformations	
Display Line Group Member DN as Connected Party	Check this check box to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

A number of new serviceability counters have been added to a folder called "Cisco Hunt Pilots" to monitor queuing. These counters, based on the Hunt Pilot DN, include:

- HuntPilot/QCallsAbandoned - the number of calls (since the last system reboot) which were queued, but disconnected, prior to being answered by a hunt member or redirected normally
- HuntPilot/CallsInQueue - the number of calls currently in queue
- HuntPilot/QCallsRingNoAnswer - the number of calls (since the last system reboot) which were not answered after being routed to a line group member
- HuntPilot/QLongestCallWaiting - the time, in seconds, of the call that currently has the longest wait time in queue
- HuntPilot/MaxQDepthExceeded - the number of occurrences (since the last system reboot) when a call was routed to an alternate destination after the maximum number of callers allowed in queue was reached
- HuntPilot/MaxQWaitTimerExceeded - the number of occurrences (since the last system reboot) when a call was routed to an alternate destination after the maximum wait time in queue was reached
- HuntPilot/LineGroupMembersAvailable - the number of idle (on-hook) line group members (DNs) currently eligible to receive calls from the queuing-enabled hunt pilot

Announcement Monitoring

The new performance counter for Media Streaming Annunciator can be reached from the Real Time Monitoring Tool via **Performance > expand server name > Cisco Media Streaming App > ANNPlayFailed**.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

NextGen mobile clients with QoE

If any device that shares the same user ID and is associated to a Hunt Group signs out of the Hunt Group, SNR calls are not sent out to the associated mobile device (RD and Mobile Clients).

Unified CM 9.0 extends the Log Out of Hunt Groups cability onto your mobile device, allowing it to function in the same way as your desk phone. After you use the Hlog softkey via your mobile client to Log Out of the Hunt Group, you no longer receive calls placed to the Hunt Pilot.

Unified CM 9.0 provides TLS/SRTP support for dual-mode smart phones. TLS establishes the same secure and reliable data transfer mode for mobile phones as for IP phones, and SRTP encrypts voice conversations.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Originally Called Party Name in Placed Call History

The following is a new chapter for the *Cisco Unified Communications Manager Features and Services Guide*.

Originally Called Party Name in Placed Call History

Cisco Unified IP Phones display call history information, which includes placed calls. For placed calls, the phone displays the dialed digits or the dialed universal resource identifier (URI), and in many cases the name of the dialed user. However, in Cisco Unified Communications Manager (Unified CM) releases earlier than Release 9.0 there were scenarios, such as Call Forwarding, in which IP phones displayed “Unknown” in the placed call history, even when the called party had a valid name configured.

In Unified CM Release 9.0 and later releases, SIP phones supporting the Originally Called Party Name in Placed Call History feature always display the name of the originally called party when the dialed party has a valid name configured and its presentation is not restricted. Unified CM provides the name to the calling SIP phone, which allows the SIP phone to populate the name in the placed call history accurately, even when a call is forwarded by the called party.

Unified CM indicates the alerting name of the originally called party to the calling SIP phone. If an alerting name is not configured for the originally called party, but the originally called party answers the call, Unified CM will send the connected display name of the originally called party if configured. If the called party has Calling Line ID Restricted (CLIR) enabled, Unified CM indicates that the name is private and the calling phone does not display name information in the placed call history.

Neither the end user nor the administrator needs to make configuration changes to enable the Originally Called Party Name in Placed Call History feature.

Intercluster calls limitations

Unified CM uses the Remote-Party-ID (RPID) header to send the alerting name of the called party. For intercluster calls, Remote-Party-ID must be enabled on the SIP intercluster trunk for the SIP phones on the calling cluster to obtain the name of the dialed party. This includes all intermediate hops involving Cisco Unified Communications Manager Session Management Edition.

On a SIP trunk, it is possible to turn off the RPID header and use only the P-Asserted-ID (PAI) or P-Preferred-ID (PPI) headers. If only PAI or PPI is used between two Unified CM clusters, the placed call history on SIP phones may not contain the display name corresponding to the dialed number or the dialed URI.

Endpoint features and behavior

The placed call history information on SIP phones will have the dialed number, or the dialed URI, and name (where available and not private). For the name of the dialed party to be displayed on the SIP phone, the alerting name must be provisioned on Unified CM and its presentation must not be restricted. For intercluster calls the ASCII alerting name must be provisioned.

Note In some cases, Cisco Unified IP Phones 8900 and 9900 Series may have the display name rather than the alerting name in the placed call history.

Note When privacy is configured only in the SIP profile of the called party device and Call Forward All (CFA), or Call Forward Busy (CFB), or Call Forward Unregistered (CFUR) is enabled, the configured alerting name is displayed rather than “private.” To ensure that “private” is displayed for call forwarding, Cisco recommends that you configure the name presentation restriction in the translation pattern or the route pattern rather than in the SIP profile.

Unified CM features and feature behavior

The Originally Called Party Name in Placed Call History feature is automatically negotiated between Unified CM and the SIP phone firmware during initial registration without requiring any configuration or administrative intervention. SIP phone firmware load 9.3.1 and higher supports the Originally Called Party Name in Placed Call History feature.

Supported phone models

The Originally Called Party Name in Placed Call History feature is supported on the following Unified IP Phones

- Cisco Unified IP Phones 6900 Series models 6921, 6941, 6945, 6961
- Cisco Unified IP Phones 7900 Series models 7906, 7911, 7931, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, 7975
- Cisco Unified IP Phones 8900 Series models 8941, 8945, 8961

- Cisco Unified IP Phones 9900 Series models 9951, 9971

SIP phone firmware load 9.3.1 and higher supports the Originally Called Party Name in Placed Call History feature.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Pause in speed dials

In Unified CM, the user can configure Forced Authorization Code (FAC), Client Matter Code (CMC), and postconnect Dual Tone Multifrequency (DTMF) digits as a part of a speed dial number. The Unified CM recognizes the destination address digits, FAC, CMC, and postconnect DTMF digits that are configured as a part of a speed dial number.

Cisco Unified Communications Manager Administration considerations

The Unified CM sends out postconnect DTMF digits with appropriate pause duration after the call is connected and a media connection is established. Even if the media connection is disconnected before a call is established, the DTMF digits are sent only after the call is connected. The user can configure the Pause in Speed Dial feature using either one of the two methods:

- Method 1: Using a comma as a pause and also as a delimiter
- Method 2: Entering destination address digits, FAC, CMC, and DTMF digits as a continuous string without using any delimiter

Bulk Administration considerations

When the user enters the phone number, it can be followed by FAC/CMC if applicable. The user can enter the phone number, FAC, CMC either in sequence or separated by a comma (,). The speed dial includes either password or any other digits to send as DTMF digits after the call is connected. If the user requires a pause while connecting through speed dial, the user can enter one or more commas (,) where each comma represents a pause of 2 seconds. While configuring a Pause in Speed Dial, the administrator must to add a label so that FAC, CMC, and DTMF digits are not displayed on the phone screen.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Record Line Key

The Record Line Key feature is an enhancement to the Call Recording feature. The following sections are either revisions to existing sections in the "Monitoring and Recording" chapter of the *Cisco Unified Communications Manager Features and Services Guide*, or new sections that were added to that chapter.

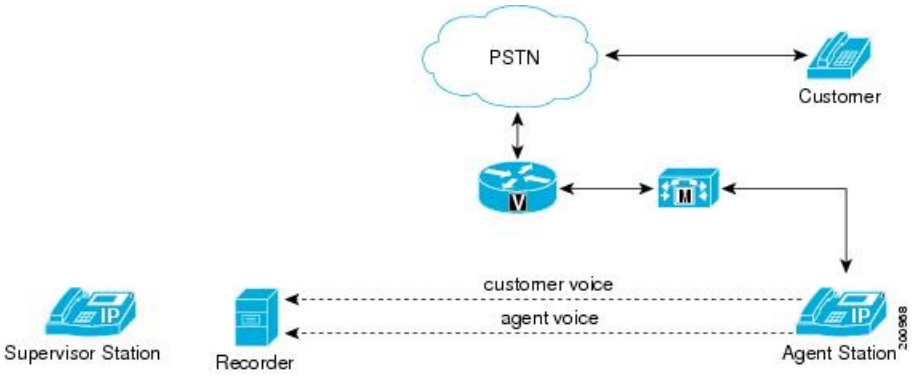
Call recording overview

Call recording is a Cisco Unified Communications Manager feature that enables a recording server to archive agent conversations. The following types of call recording exist:

- Automatic recording—All agent calls are recorded automatically.
- Selective recording—Only selected agent calls are recorded.

The following figure illustrates call recording.

Figure 4: Call recording overview



Determine device support for call monitoring and call recording

For a complete list of devices that support both the silent monitoring and call recording features, see http://developer.cisco.com/web/sip/wikidocs.

Recorders

Recorders must interface with Cisco Unified Communications Manager SIP trunk to receive recording calls. Consult with the recording vendor to determine which third-party recording applications and versions support the call recording feature.

Call recording modes

The following modes of call recording exist:

- Automatic call recording—In automatic call recording, the recording session automatically establishes when the agent call connects.
- Selective call recording—In selective call recording, recording can be initiated using a softkey or programmable line key assigned to the device, a CTI-enabled application, or both interchangeably.

Note In all call recording modes, the agent call must be active before call recording takes place.

The administrator configures the recording option and recording profile on the agent line appearance. By default, the recording option specifies Call Recording Disabled.

When the recording option is set to either Automatic Call Recording Enabled or Selective Call Recording Enabled, the line appearance can be associated with a recording profile. The recording profile specifies the following parameters: Recording Calling Search Space and Recording Destination Address.

When automatic call recording is enabled, start and stop recording requests using a softkey, programmable line key, or CTI-enabled application are rejected.

CTI requirements

Computer Telephony Integration (CTI) provides the ability for applications to monitor calls on a per-call basis. Cisco defines the monitor target as the party that is monitored and the monitor initiator as the monitoring party.

If a single application observes both the monitor target and the monitor initiator, call events that get reported to the application help the application identify calls on the monitor target and provide the ability to monitor the calls. If different applications observe the monitor target and the monitor initiator, the application that observes the monitor target must provide the call information to the application that observes the monitor initiator. Based on the call information that is available to the application that observes the monitor initiator, a monitoring request can get initiated. Termination of the call at the monitor initiator or monitor target stops the monitoring session.

For recording, Cisco Unified Communications Manager provides the ability to record all calls automatically. The SIP or SCCP station initiates this automatic recording and is based on configuration of Cisco Unified Communications Manager Administration. Administrators can configure no recording, automatic recording of all calls, or selective recording for a line appearance. In selective call recording, recording can be initiated using a softkey or programmable line key assigned to the device, a CTI-enabled application, or both interchangeably. CTI does not provide the ability to override the administrator configuration in the database.

Selective recording supports two modes: silent recording and user recording.

In the silent recording mode the call recording status is *not* reflected on the Cisco IP device display. Silent recording is typically used in a call center environment to enable a supervisor to record an agent call. A CTI-enabled application running on the supervisor desktop is generally used to start and stop the recording for the agent-customer call.

In the user recording mode the call recording status is reflected on the Cisco IP device display. A recording may be started or stopped using a softkey, programmable line key, or CTI-enabled application running on the user desktop.

When invoking recording and monitoring or any other CTI features, delays and unexpected behavior can result if UDP transport is used for phones that are running SIP.

Applications that intend to monitor or record calls should have the corresponding monitoring and recording privileges enabled for the application user or end user that the application uses.

For convenience the MonitoringPartyInfo, MonitoredPartyInfo, and RecordPartyInfo all get combined and reported as CallAttributeInfo from CTI to applications.

Selective call recording

This section provides detailed call flows and explanations of the use cases when an agent device is configured for selective call recording. For more information about automatic call recording use cases, see the "Monitoring and Recording" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

In selective call recording, recording can be initiated using a softkey or programmable line key assigned to the device, a CTI-enabled application, or both interchangeably.

Selective call recording supports two modes:

Silent recording

In the silent recording mode the call recording status is *not* reflected on the Cisco IP device display. Silent recording is typically used in a call center environment to enable a supervisor to record an agent call. A CTI-enabled application running on the supervisor desktop is generally used to start and stop the recording for the agent-customer call.

User recording

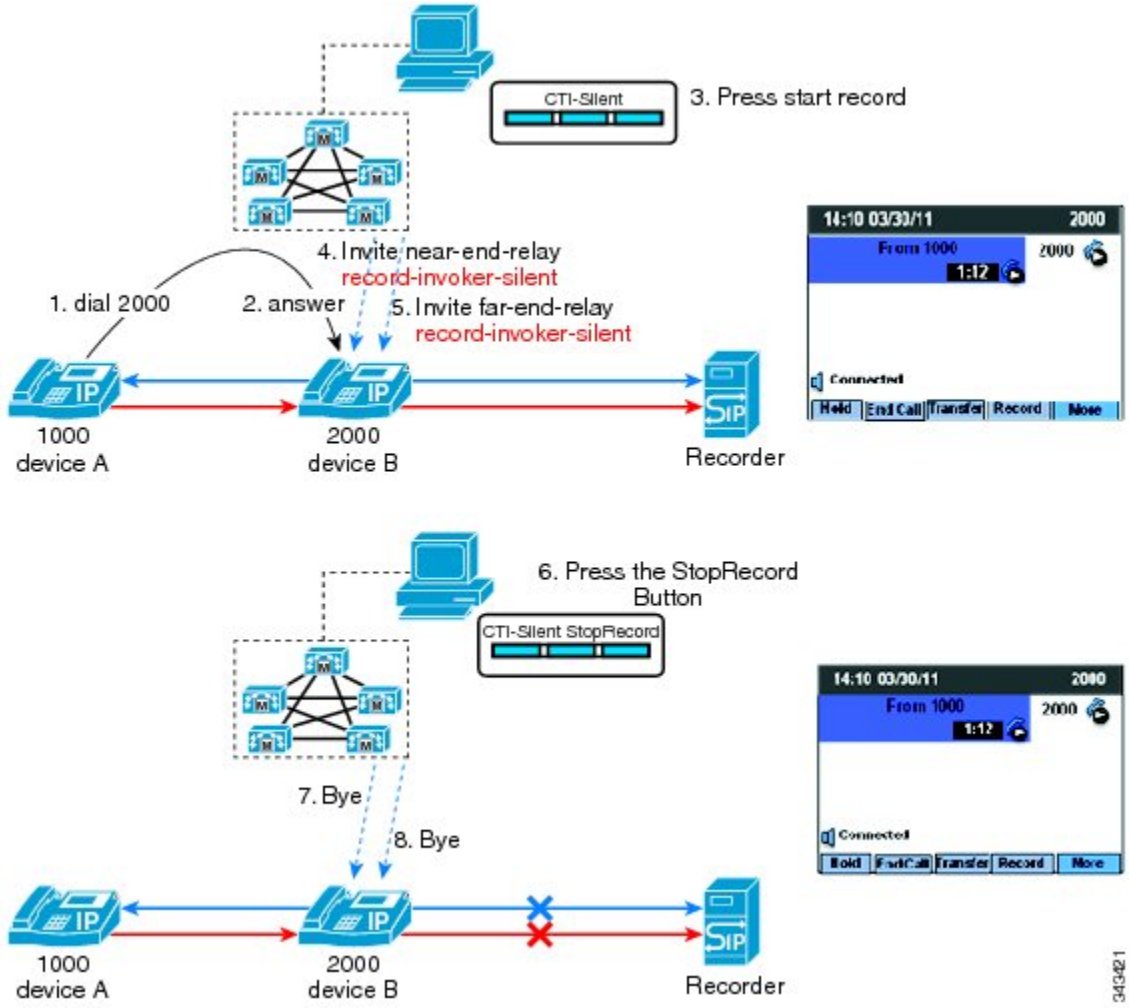
In the user recording mode the call recording status is reflected on the Cisco IP device display. A recording may be started or stopped using a softkey, programmable line key, or CTI-enabled application running on the user desktop.

Selective call recording—silent recording mode

In this use case for selective call recording—silent recording mode, the supervisor manages the recording session from a CTI-enabled desktop.

The following figure illustrates selective call recording—silent recording mode.

Figure 5: Selective call recording—silent recording mode



In this use case:

- Device A (DN 1000) calls device B (DN 2000).
- The user on device B answers the call.
- The supervisor uses a CTI-enabled application to start and stop the call recording session.

The supervisor starts the recording session using a CTI-enabled desktop. Cisco Unified Communications Manager makes two recording calls to the built-in bridge (BIB) of the Cisco IP device (one call for the near-end media; another call for the far-end media). The recording calls are automatically and silently answered.

Cisco Unified Communications Manager extends both recording calls to the recording server connected by a SIP trunk.

The recorder receives and answers both recording calls and the user Cisco IP device starts to fork both media streams to the recorder. The call recording status is not reflected on the Cisco IP device display.

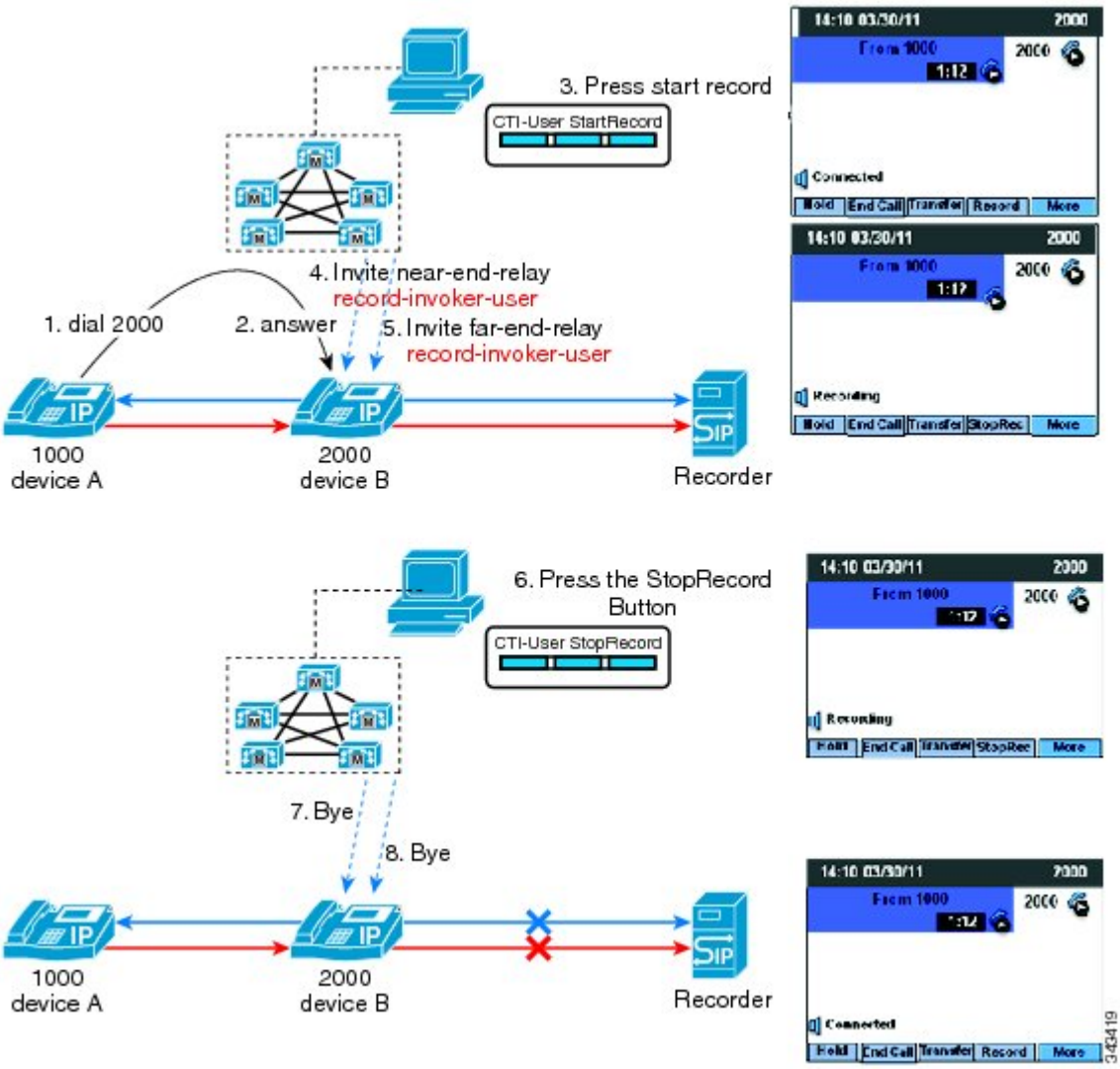
The CTI-enabled application is used to stop the recording session. Cisco Unified Communications Manager clears both recording calls.

Selective call recording user recording mode—recording session managed from a CTI-enabled application

In this use case for selective call recording—user recording mode, the user manages the recording session from a CTI-enabled desktop.

The following figure illustrates selective call recording user recording mode—recording session managed from a CTI-enabled application.

Figure 6: User recording mode managed from a CTI-enabled application



In this use case:

- Device A (DN 1000) calls device B (DN 2000).

- The user on device B answers the call.
- The user on device B uses a CTI-enabled application to start and stop the call recording session.

The user starts the recording session using a CTI-enabled desktop. Cisco Unified Communications Manager makes two recording calls to the built-in bridge (BIB) of the Cisco IP device (one call for the near-end media; another call for the far-end media). The recording calls are automatically and silently answered.

Cisco Unified Communications Manager extends both recording calls to the recording server connected by a SIP trunk.

The recorder receives and answers both recording calls and the user Cisco IP device starts to fork both media streams to the recorder. The Cisco IP device display updates to reflect *Recording*. The key toggles from *Record* to *StopRec*.

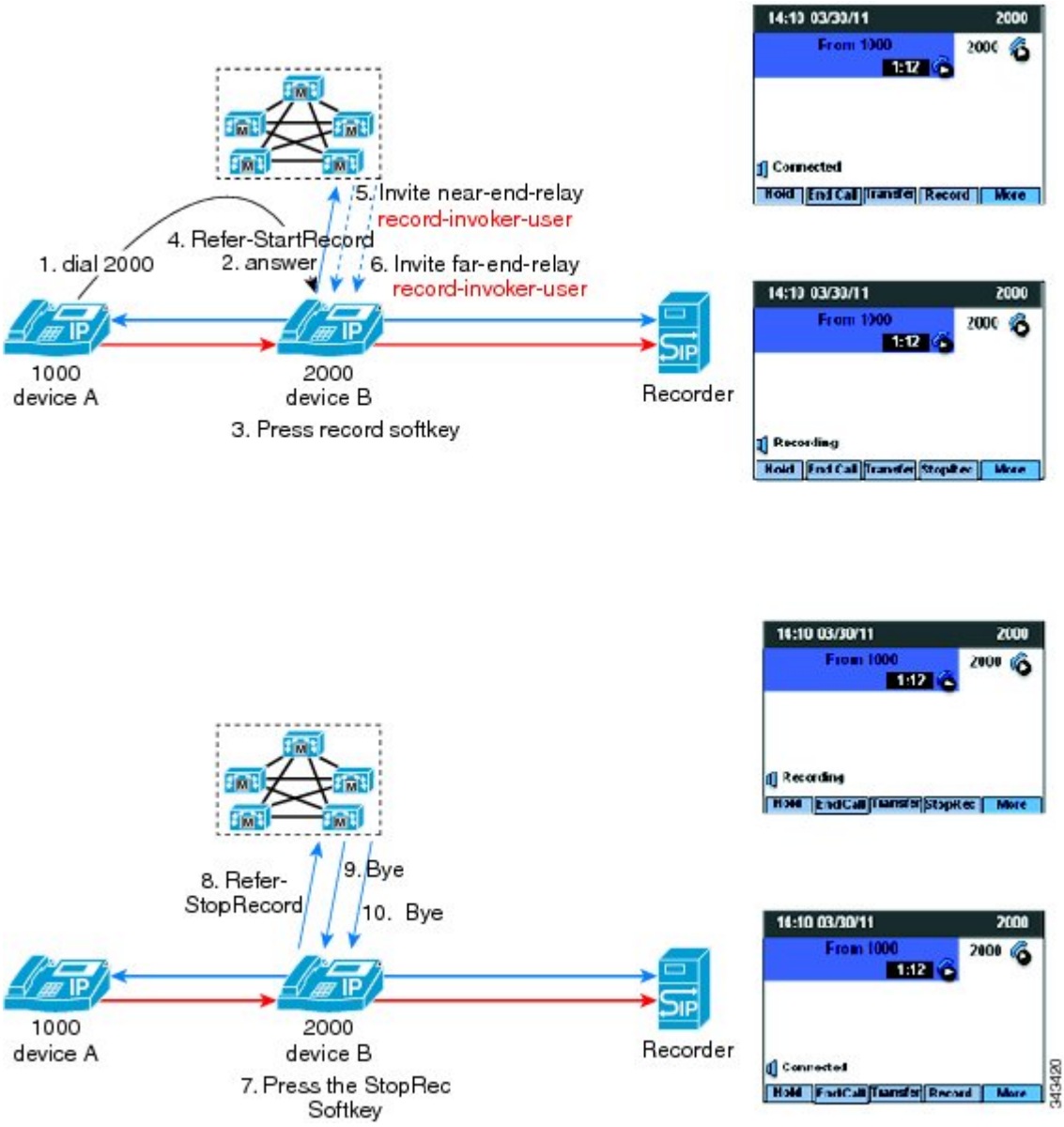
The CTI-enabled application is used to stop the recording session. Cisco Unified Communications Manager clears both recording calls.

Selective call recording user recording mode—recording session managed from a Cisco IP device

In this use case for selective call recording—user recording mode, the user presses a softkey or programmable line key on a Cisco IP device to start and stop the call recording session.

The following figure illustrates selective call recording user recording mode—recording session managed from a Cisco IP device.

Figure 7: User recording mode managed from a Cisco IP device



In this use case:

- Device A (DN 1000) calls device B (DN 2000).
- The user on device B answers the call.
- The user on device B uses the softkey or programmable line key on the Cisco IP device to start and stop the call recording session.

The user presses the *Record* key to start the recording session. Cisco Unified Communications Manager makes two recording calls to the built-in bridge (BIB) of the Cisco IP device (one call for the near-end media; another call for the far-end media). The recording calls are automatically and silently answered.

Cisco Unified Communications Manager extends both recording calls to the recording server connected by a SIP Trunk.

The recorder receives and answers both recording calls and the user Cisco IP device starts to fork both media streams to the recorder. The Cisco IP device display updates to reflect *Recording*. The key toggles from *Record* to *StopRec*.

The User presses the *StopRec* key to stop the recording session.

Cisco Unified Communications Manager clears both recording calls.

Additional information

For additional information on the Record Line Key feature, refer to the "Monitoring and Recording" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Cisco Unified Communications Manager Administration considerations

The following table describes the Recording Option field in the **Directory Number Configuration** window.

Table 7: Directory number configuration settings

Field	Description
Recording Option	This field determines the recording option on the line appearance of an agent. The default recording option is Call Recording Disabled. Choose one of the following options: • Call Recording Disabled—Calls made on this line appearance cannot be recorded. • Automatic Call Recording Enabled—Calls made on this line appearance are recorded automatically. • Selective Call Recording Enabled—Calls made on this line appearance can be recorded using a softkey or programmable line key that is assigned to the device, a CTI-enabled application, or both interchangeably. Selective recording supports two modes: • Silent recording—Call recording status is not reflected on the Cisco IP device display. Silent recording is typically used in a call center environment to allow a supervisor to record an agent call. A CTI-enabled application running on the supervisor desktop is generally used to start and stop the recording for an agent-customer call. • User recording—Call recording status is reflected on the Cisco IP device display. A recording can be started or stopped using a softkey, programmable line key, or CTI-enabled application running on the user desktop. To enable user recording, add the Record softkey or programmable line key to the device template. Do not add the Record key if only silent recording is desired. When the recording option is set to either Automatic Call Recording Enabled or Selective Call Recording Enabled, the line appearance can be associated with a recording profile. When automatic recording is enabled, start- and stop-recording requests using a softkey, programmable line key, or CTI-enabled application are rejected.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

Procedures

Set up Monitoring and Recording

Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. To protect themselves from legal liability, call centers need to be able to archive agent-customer conversations.

The silent call monitoring feature allows a supervisor to eavesdrop on a conversation between an agent and a customer; neither the agent nor the customer can hear the supervisor voice. The call recording feature allows system administrators or authorized personnel to archive conversations between the agent and the customer.

Perform the following steps to set up monitoring and recording.

Procedure

Step 1 Turn on IP phone BIB to allow monitoring or recording.
Step 2 Add user for monitoring or recording application.
Step 3 Add user to groups that allow monitoring and recording.
Step 4 Optional. Configure tones for monitoring or recording.
Step 5 Configure DN for a monitoring calling search space.
Step 6 Enable recording for a line appearance.
Step 7 Optional. Add the Record softkey or programmable line key to the device template.
Step 8 Create a recording profile.
Step 9 Optional. Create a SIP profile for recording.
Step 10 Create a SIP trunk that points to the recorder.
Step 11 Create a route pattern for the recorder.
Step 12 Configure recorder redundancy.

Add the Record softkey or programmable line key to the device template (optional)

To enable a user to start and stop recording from a Cisco IP device, add the Record softkey or programmable line key to the device template.

To add the Record softkey, use the **Device > Device Settings > Softkey Template** menu option in Cisco Unified Communications Manager Administration to create or modify a nonstandard softkey template. Configure the softkey layout for call state *connected* to have the Record softkey in the selected softkeys list.

To add the Record programmable line key, use the **Device > Device Settings > Phone Button Template** menu option in Cisco Unified Communications Manager Administration. Enter the button template name, feature, and label.

Enable recording for a line appearance

To enable recording of an agent, set the Recording Option in the line appearance of the agent to one of the following options:

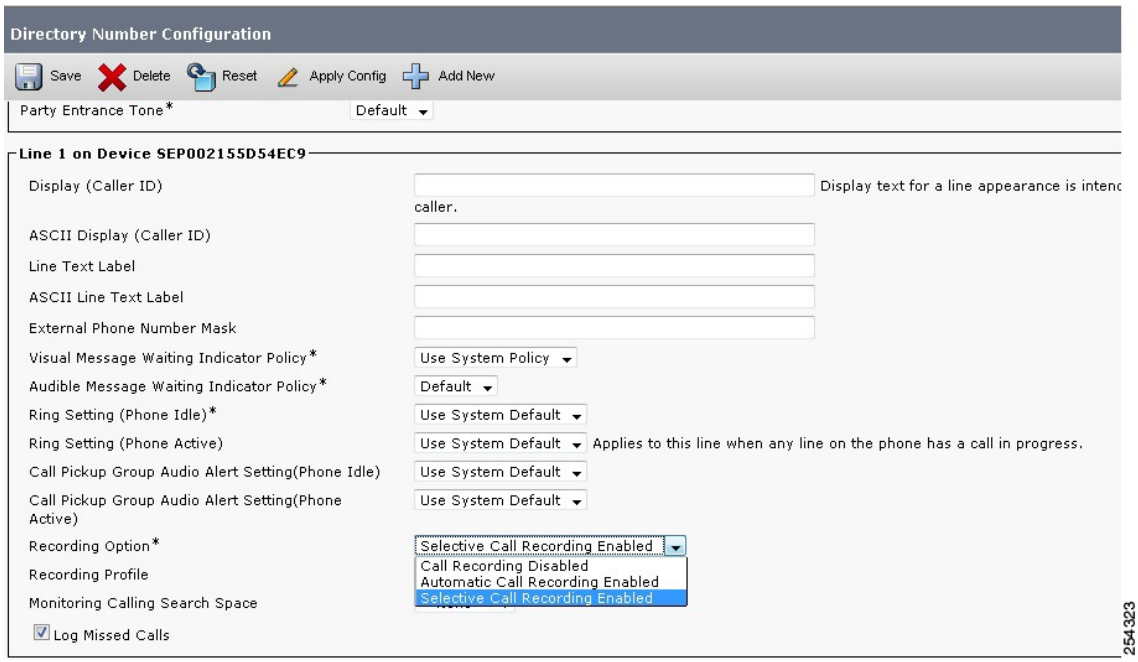
- Automatic Call Recording Enabled
- Selective Call Recording Enabled

Select a pre-created recording profile from the drop-down list box. (**Use Device** > **Device Settings** > **Recording Profile** to configure a recording profile.)

Use the Call **Routing** > **Directory Number** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

The following figure illustrates enabling recording for a line appearance.

Figure 8: Enabling Recording for a Line Appearance



Additional information

For more information about the other steps in Set up Monitoring and Recording, on page 101, see the Monitoring and Recording chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

CLI changes

No changes.

Secure Adhoc Conference MCU Setup

Cisco Unified Communications Manager supports secure video conferencing using a Cisco TelePresence MCU as the conference bridge. Cisco Unified Communications Manager and Cisco TelePresence MCU can be set up to use SRTP to encrypt all media in the video conference.

To ensure that the video conference is secure, you must set up a TLS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU so that you do not expose keys and other security-related information during call negotiations.

Cisco Unified Communications Manager Administration considerations

A number of changes have been made to the Conference Bridge Configuration menu that can be accessed by choosing the **Media Resouces** > **Conference Bridge** menu path, and then choosing **Cisco TelePresence MCU** from the Conference Bridge Type drop-down list box.

The following fields have been removed from the Conference Bridge Configuration window for Cisco TelePresence MCU::

- Unified CM SIP Port

The following fields have been added to the Conference Bridge Configuration window for Cisco TelePresence MCU:

- SIP Profile—From the drop-down list box, choose the Standard SIP Profile for TelePresence Conferencing
- SIP Trunk Security Profile—From the drop-down list box, choose the security profile to apply to the SIP trunk.
- SRTP Allowed—Check this check box to enable encrypted media with SRTP.
- Script—From the drop-down list box, choose the normalization script that you want to apply to Cisco TelePresence MCU.
- Enable Trace—Check this check box to enable tracing within the script or uncheck this check box to disable tracing.
- Parameter Name/Parameter Value—In these text boxes you can enter parameter names and values for your normalization script.
- Use HTTPS—Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU. The default HTTPS port is 443.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

You must configure a TLS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU so that you do not expose keys and other security-related information during call negotiations.

Serviceability considerations

No changes.

Procedures

Set up TLS connection with Cisco TelePresence MCU

If you are using SRTP with Cisco TelePresence MCU, you must set up a TLS connection with Cisco TelePresence MCU so that you do not expose keys and other security-related information during call negotiations.

Note This procedure details tasks that are performed in Cisco Unified Communications Manager. For detailed instructions on how to import and export certificates in Cisco TelePresence MCU, see your Cisco TelePresence MCU product documentation.

Procedure

Step 1 Download the Cisco Unified Communications Manager security certificate by performing the following steps:

a) In Cisco Unified Operating System Administration, choose **Security** > **Certificate Management.**
b) Click **Find**.
c) Click **CallManager.pem** to view the certificate.
d) Click **Download** and save the file to a local drive.

Step 2 Upload the Cisco Unified Communications Manager certificate to Cisco TelePresence MCU.

Step 3 Generate self-signed certificates for Cisco TelePresence MCU and save the certificates to a local drive.

Step 4 Upload self-signed certificates to the Cisco TelePresence MCU.

Step 5 Upload Cisco TelePresence MCU certificates to Cisco Unified Communications Manager by doing the following:

a) In Cisco Unified Operating System Administration, choose **Security** > **Certificate Management**.
b) Click **Upload Certificate/Certificate Chain**.
c) From the Certificate Name drop-down list box, choose **CallManager-trust**.
d) Click **Browse** and locate the Cisco TelePresence MCU certificate that you saved locally.
e) Click **Upload File** to upload certificates.

Step 6 In Cisco Unified Communications Manager Administration, choose **System** > **Security** > **SIP Trunk Security Profile** and create a secure SIP Trunk Security Profile that uses the following settings:

- Device Security Mode must be Encrypted
- Incoming Transport Type and Outgoing Transport Type must be TLS
- X.509 Subject Name must be set to the defined Common Name that is used in the Cisco TelePresence MCU certificates

Step 7 On the Cisco TelePresence MCU, configure SIP signaling encryption with TLS, and media encryption with SRTP.

CLI changes

No changes.

Secure Cross Cluster Extension Mobility

The Cisco Extension Mobility Cross Cluster feature allows an enterprise user of one Cisco Unified Communications Manager cluster (the home cluster) to log in to a Cisco Unified IP Phone of another Cisco Unified Communications Manager cluster (the visiting cluster) during travel as if the user is using the IP phone at the home office.

Cisco Unified Communications Manager Administration considerations

EMCC and security mode among clusters of different versions

This section lists the interactions of the Cisco Extension Mobility Cross Cluster with different versions and security modes.

Note Phone configuration files can be encrypted only if both the home cluster and visiting cluster versions are in 9.x, and when the TFTP encryption configuration flag is enabled.

During EMCC login, if both the visiting cluster and home cluster versions are in 9.x, the phone will behave in various modes as shown in the following table.

Table 8: Supported security modes when both visiting cluster and home cluster are in 9.x versions

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
9.x	Mixed	9.x	Mixed	Secure	Secure EMCC
9.x	Mixed	9.x	Mixed	Nonsecure	Nonsecure EMCC
9.x	Mixed	9.x	Nonsecure	Nonsecure	Nonsecure EMCC
9.x	Nonsecure	9.x	Mixed	Secure	Login fails
9.x	Nonsecure	9.x	Nonsecure	Nonsecure	Nonsecure EMCC

During EMCC login, if the visiting cluster version is 8.x and the home cluster version is 9.x, the phone will behave in various modes as shown in the following table.

Table 9: Supported security modes when visiting cluster is in 8.x and home cluster is in 9.x version

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
9.x	Mixed	8.x	Mixed	Secure	Not supported
9.x	Mixed	8.x	Mixed	Nonsecure	Nonsecure EMCC
9.x	Mixed	8.x	Nonsecure	Nonsecure	Nonsecure EMCC
9.x	Nonsecure	8.x	Mixed	Secure	Not supported
9.x	Nonsecure	8.x	Nonsecure	Nonsecure	Nonsecure EMCC

During EMCC login, if the visiting cluster version is 9.x and the home cluster version is 8.x, the phone will behave in various modes as shown in the following table.

Table 10: Supported security modes when visiting cluster is in 9.x and home cluster is in 8.x version

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
8.x	Mixed	9.x	Mixed	Secure	Login fails
8.x	Mixed	9.x	Mixed	Nonsecure	Nonsecure EMCC

8.x	Mixed	9.x	Nonsecure	Nonsecure	Nonsecure EMCC
8.x	Nonsecure	9.x	Mixed	Secure	Login fails
8.x	Nonsecure	9.x	Nonsecure	Secure	Nonsecure EMCC

Error Codes for the Cisco Extension Mobility Service (EMService)

The following table lists and describes the error codes that apply to the Cisco Extension Mobility service (EMService).

Table 11: Error Codes for the Cisco Extension Mobility Service (EMService)

Error Code	Phone Display	Quick Description	Description
43	Login is unavailable(43)	Device Security mode error	Device Security Profile associated to the EMCC device should be Non Secure for its Device Security Mode. **Note** This error code does not apply for Cisco Unified Communications Manager Release 9.x and above.
45	Login is unsuccessful(45)	Remote Cluster version not supported	Occurs during EMCC login when the visiting cluster version is 9.x and is in mixed mode, the phone is in secure mode, and the home cluster version is 8.x.
46	Login is unsuccessful(46)	Remote Cluster security mode not supported	Occurs during EMCC login when the visiting cluster security mode is in mixed mode, the phone is in secure mode, and the home cluster is in nonsecure mode.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

EMCC and Security Mode Among Clusters

- Clusters can be nonsecure or mixed-mode clusters.
- Phones that allow Cisco Extension Mobility Cross Cluster can be in secure and nonsecure mode.

Serviceability considerations

No changes.

CLI changes

No changes.

Serviceability for locations CAC enhancements

This feature enables an administrator to view details of the configured locations in an enterprise, understand the link and intralocation discrepancies, view the effective path between the two locations, and identify disconnected groups of locations.

Locations Topology

Cisco Unified Serviceability Locations Topology (**Tools** > **Locations** > **Topology Report**) provides details of configured locations in your enterprise. Location Topology refers to a modeled topology representing the flow of media in a network.

Listed below are some commonly used terms and their definitions:

Assertion

An assertion refers to the location and link bandwidth and weight values configured in a cluster. Asserted values may be replicated to another cluster.

Discrepancy

A discrepancy occurs if there is a difference in the location bandwidth values, link bandwidth values, or link weight values asserted across various clusters.

Effective Path

An effective path is a sequence of intermediate locations connecting two end locations, with weight and bandwidth allocations assigned to each link between each adjacent pair of locations. The effective path, as determined by the least cumulative weight, is the only path used for bandwidth deductions between any two end locations.

Locations Discrepancy

The Locations Discrepancy screen (**Tools** > **Locations** > **Discrepancy Report**) displays the conflicts in assertions for various locations configurations.

The following details are displayed:

- Link Configuration Discrepancy—Includes the discrepancy details of the link connecting two locations such as weight, audio, video and immersive bandwidth.
- Intralocation Configuration Discrepancy—Includes intralocation discrepancy details such as audio, video, and immersive bandwidth.

Effective Path

The Cisco Unified Serviceability Effective Path screen (**Tools** > **Locations** > **Effective Path**) provides details of the effective path that media take for audio, video, or immersive calls made between two locations provided by the administrator. This screen displays the Available bandwidth (Available bandwidth = Configured bandwidth – Used bandwidth) and the Configured bandwidth across each link and intralocation in the effective path. An administrator can use this report to determine bandwidth availability across a link and intralocation when there are bandwidth issues in making calls. Cisco Unified Serviceability Effective Path can also be used to troubleshoot bandwidth issues in making calls and find out where the bandwidth availability is low.

The Cisco Unified Serviceability Effective Path screen displays the following details between two selected locations:

- Quick Path Overview —Displays the Cumulative Weight and the least of the configured and available audio, video, and immersive bandwidth values across the effective path.
- Detailed Path View—Displays the weight and bandwidth values (Available and Configured) for Audio, Video, and Immersive calls for locations and links constituting the effective path, in a tabular view ordered from source location at top to the destination location at bottom.

Note The Available Bandwidth values displayed in the report are the values at the time of viewing the effective path. You can view the real-time values in the Cisco Unified Real-Time Monitoring Tool.

Disconnected Groups

Cisco Unified Serviceability Disconnected Groups screen (**Tools** > **Locations** > **Disconnected groups**) enables an administrator to view and analyze any disconnect between the locations that are part of the topology. It displays a list of disconnected groups of locations, which helps an administrator understand which locations must be connected.

The disconnect in the topology can occur when a link between two locations is not configured or a shared location name is misspelled.

Note The Disconnected Groups screen only displays and compares disconnected groups of locations. For information on connecting locations, see the "Location Configuration" chapter in *Cisco Unified Communications Manager Administration Guide*.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

A new submenu has been added under Tools menu (**Tools** > **Locations**).

The Locations submenu consists of the following:

- Topology Report (**Tools** > **Locations** > **Topology Report**)
- Discrepancy Report (**Tools** > **Locations** > **Discrepancy Report**)
- Effective Path (**Tools** > **Locations** > **Effective Path**)
- Disconnected Groups (**Tools** > **Locations** > **Disconnected Groups**)

Procedures

View locations topology

Cisco Unified Serviceability Locations Topology helps an administrator view the graphical locations topology in a tabular format. The administrator can filter required location names using the **Find** filter. The locations topology data includes the intralocation details and link details for a selected location.
This section describes how to search and view location topology in Cisco Unified Serviceability.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Locations** > **Topology**
The Locations Topology window appears.

Step 2 From the Find Locations Where Location Name drop-down box, choose the filter criteria.

Step 3 Enter the search string in the Find Locations Where Location Name field and then click Find.

Note The Find Locations Where Location Name field is not case-sensitive.

The list of locations is displayed for the chosen filter criteria.

Step 4 In the list, click to expand any location to view its intralocation details and link details.
The intralocation details include audio, video, and immersive bandwidth whereas the link details contain the details of the link connecting two locations such as its weight, audio, video and immersive bandwidth.

Tip If the list of locations is long, it may run into multiple pages. To view another page, click the appropriate navigation button at the bottom of the Locations Topology window or enter a page number in the Page field. To change the number of locations that display in the window, choose a different value from the Rows Per Page drop-down box.

Tip If a location is highlighted by a Caution symbol, this indicates a discrepancy. To view the details of this discrepancy, click **View Assertion Details** link.

Step 5 To view the assertion details of any location, click **View Assertion Details** link at the bottom of the expanded details section.
The Assertion Details window appears.

Step 6 To return to the Locations Topology window, click **Close.**

Note To download the locations topology data in xml format, click **Download Topology** at the bottom of the Locations Topology window or **Download Topology** icon in the toolbar at the top.

For more information about the topology data in xml format, refer Cisco Unified Communications Manager XML Developers Guide.

View locations discrepancy

This section describes how to view a location discrepancy in Cisco Unified Serviceability.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Locations** > **Discrepancy**.
The Location Discrepancy window appears.

Step 2 The list of link configuration discrepancies and intralocation configuration discrepancies is displayed.

Note The Link Configuration Discrepancy section lists only those link names where discrepancy has been detected. Link names are listed in the format <*Location Name 1*> <--> <*Location Name 2*>. The Intralocation Configuration Discrepancy section lists only those location names where such discrepancy has been detected. The elements in the list are sorted in lexical order.

If no discrepancies are found, the following status message is displayed:

```
No discrepancies found
```

Step 3 In the list, click on a link name or location name to expand and view its configuration details as asserted by different clusters, in a tabular view.
The bottom row displays the effective values considered for audio, video, and immersive bandwidth pools and weight (in the case of links). The values that do not match with the effective values are highlighted in red.

Note The Effective Value is the least of the values in a particular column. For example, the Effective Value of audio bandwidth is the minimum value in the Audio Bandwidth column.

View effective path

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Locations** > **Effective Path**.
The Effective Path window appears.

Step 2 From the **Location** drop-down boxes, select any two locations between which effective path is required and then click **Find.**
Alternatively, start typing the location name in the input box to shortlist the matching location names and then click **Find.**

The Effective path details which include the Quick Path Overview and Detailed Path View sections are displayed. If there is no path between the two selected locations, the following status message is displayed:

```
No path exists between <From_Location> and <To_Location>.
```

View disconnected groups

This section describes how to view disconnected groups in Cisco Unified Serviceability.

- ◦ In Cisco Unified Serviceability, choose **Tools** > **Locations** > **Disconnected Groups**.

  The Disconnected Groups screen appears.

The following table describes the settings displayed on the Disconnected Groups screen.

Table 12: Settings on the Disconnected Groups screen

Setting	Description
List of Disconnected Groups	
Select	Check this box to select a disconnected group to be compared with another disconnected group. **Caution** You can select only two groups for comparison.
Group ID	Auto-generated unique identification number of the selected group is displayed here.
Description	The names of the first and last location in alphabetical order in the group are displayed here. **Note** If a disconnected group has only one node, only the name of that node is displayed here.
No. of Locations	The number of locations in a group is displayed here.

Setting	Description
Compare Selected Groups	Click this button to display and compare the selected groups. After you click this button, the details pertaining to the selected groups are displayed. For every group you select, names of the locations that are part of that group and the corresponding clusters that assert a location are displayed. See Comparison view for the selected groups, below.
Comparison view for the selected groups	
Location Name	The names of all the locations that are part of a group are listed in this column.
Asserted by Cluster	The names of all the clusters that assert a particular location are listed in this column.

If there are no disconnected groups of locations, the following status message is displayed:

```
No disconnected groups of locations found
```

Note The List of Disconnected Groups can be sorted by any column. By default, the groups are sorted by the No. of Locations column.

CLI changes

No changes.

Session Trace enhancement

For Cisco Unified Communications Manager 9.0 and later, you can use Cisco Unified Real-Time Monitoring Tool (RTMT) to upload the call logs to your local system. Based on the uploaded call logs, RTMT can search for the matching calls, list the matching records, and provide SIP Message Call Flow Diagrams.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

The Call Process menu contains the following updates:

- **CallManager** > **Call Process** > **Session Trace Log View**—The Session Trace submenu has been renamed as Session Trace Log View.
- **CallManager** > **Call Process** > **Session Trace Log View** > **Monitor Real-Time Data**—All the fields that were available under Session Trace submenu are now available in Monitor Real-Time Data window.
- **CallManager** > **Call Process** > **Session Trace Log View** > **Review from Provided Logs**—A new window has been added which contains the following fields:
  - File Location—To specify the directory where the call log files are stored
  - Enable Time Based Search— To view call records for a specific duration
  - Duration—To specify the duration for which calls need to be reviewed

Security considerations

No changes.

Serviceability considerations

No changes.

Procedures

Open from local disk

The following procedure describes the steps to monitor session trace data from the logs saved on your local disk:

Procedure

	Command or Action	Purpose
Step 1	From the RTMT menus, choose **CallManager** > **Call Process** > **Session Trace Log View** > **Open from Local Disk**.	The Open from Local Disk screen appears.
Step 2	In the **File Location** field, specify the directory where the call log files are saved on	

	Command or Action	Purpose
	your local disk. You can click **Browse** to specify the directory path.	
Step 3	Check the **Enable Time Based Search** check box to view call records for a specific duration. If you check this check box, you can specify the duration in **Duration** field. If you do not check this check box, you will not be able to specify the duration. In such cases, all the calls from the specified Start Time that are present in the saved log files will be displayed.	
Step 4	Enter the search criteria and click **Run.**	**Note** In Calling Number/URI, Called Number/URI, you can use the wildcard character '*' to match any number of characters. For example, a search for 123* fetches numbers like 123, 1234, 123456, 123*, and so on. 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, Calling Device Name, Called Device Name, and Termination Cause Code. **Note** The Called Party Trace Feature adds the Calling Device Name and Called Device Name fields. **Note** If cause code description is missing or if you want more information about the Termination Cause Codes, refer the CDR cause codes in *Cisco Unified Call Details Records Administration Guide*.

CLI changes

No changes.

SIP CLI handling change

Unified CM provides a SIP feature that delivers two sets of calling party identities for outgoing SIP calls, and allows selective CLI (Calling Line Identification) for incoming SIP calls based on SIP headers.

Outgoing SIP Call with two sets of Identities

When switch-board data is configured on a SIP Trunk, the original caller identification is not overwritten by the data in the SIP headers, for the outgoing sip messages, when the **Maintain Original Caller ID DN** and **Caller Name in Identity Headers** are checked.

Outgoing SIP Call with two set of Identities - SIP Line

When Maintain Original Caller ID DN and Caller Name in Identity Headers are configured on the SIP Trunk, all outgoing SIP calls are impacted. This feature can also be configured for groups of SIP line devices via SIP Profiles. On the phone section of the SIP profile page, two new text boxes were added named **Caller ID DN** and **Caller Name** to mirror the switch-board data on a SIP Trunk. On the trunk section of SIP profile a new check box was added called **Allow Passthrough of Configured Line Device Caller Information**.

Incoming CLI for SIP Calls

Unified CM allows you to enhance identity selection, presentation and restriction on SIP interfaces. The addition of new configuration fields used for presentation on the SIP Trunk as well as on the SIP profiles to control corresponding SIP phones provides this new functionality.

With the introduction of the Outgoing Identity feature, an incoming SIP call can have two sets of calling party identities. Incoming CLI (Calling Line Identification) was introduced to aid in selecting the identity for call processing. Selection is controlled via a new list box for Calling Line Identification Presentation.

In some networks, there are two sets of identities maintained, network provided identity (trusted) and user provided identity (nontrusted). In terms of SIP calls, identity headers including P-Asserted-Identity (PAI), P-Preferred-Identity (PPI) and Remote-Party-ID (RPID) carry the network provided identity, while the FROM header carries the user provided identity. Previous releases of Unified CM provided only a single set of identities for outgoing calls. The identities in the identity headers and FROM headers were exactly the same and there was no way to differentiate between the network-provided identity and the user provided identity. Typically, the administrator configures each user device with a Directory Number (DN) and a display name. An outgoing call from this DN would carry its directory number and display name in both Identity headers and the From header. Administrators can also configure another identity on a SIP trunk. This identity, sometimes called a switchboard identity, is used to hide each individual caller's identity. It can be configured on the Caller Information section of a SIP Trunk for outbound calls. The configuration includes two fields, **Caller ID DN** and **Caller Name**. The caller's original directory number and display name are overwritten when such configurations are enabled.

Unified CM 9.0 provides configurations where the administrator can enable both the switchboard identity and original caller identity. The switchboard identity is carried in the FROM header and original caller identity will be carried in Identity headers. Such configuration can be enabled for each SIP Trunk or SIP user device.

For the incoming calls from within the network, Unified CM provides configurations to accept the network provided identity carried in Identity headers or the user provided identity carried in FROM header. Unified CM maintains a single set of identities per call.

Note As of Unified CM 7.0.1, three different identity headers are supported, PAI, PPI and RPID. Depending on the Call Routing Information configuration on the SIP trunk page, one or two of these headers may be present in an outgoing request or response.

Outgoing Call with Original Caller Identity is configured by default in the Call Routing Information. By default the **Remote-Party-Id** and **Asserted-Identity** check boxes are checked and the **Asserted-Type** and **SIP Privacy** fields are set to Default.

To configure an outgoing call with the switchboard identity, set the Caller ID DN and Caller Name on the Calls section of SIP Trunk configuration page. These provide the switchboard identity and hide the caller's identity.

For calls originated from Unified CM devices, the Identity headers are set to the line ID of the device and the From header is set to either the same as the Identity header or the switchboard information. This is provision-able and does not require changes in Unified CM. On the SIP Trunk Configuration page, there is a new check box for **Maintain Original Caller ID DN** and **Caller Name in Identity Headers** which is used to control the display name and number of outgoing SIP messages. When enabled for the outgoing SIP messages, the configured value Caller ID DN will not override the phone number and the configured Caller Name will not overwrite the caller name in outgoing Identity headers.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

SIP Diversion Counter

The following is a new chapter for the *Developer Guide for SIP Transparency and Normalization*.

Preloaded scripts

Preloaded scripts are Lua scripts that are provided as part of a Cisco Unified Communications Manager (Unified CM) basic installation. The preloaded scripts are automatically available when you upgrade to (or install) Unified CM Release 8.6 or a later release. These scripts normally have transparency- and normalization-related Lua code that you can use for a particular feature and are named with an easy-to-follow naming convention.

The administrator can select the preloaded scripts on the SIP Trunk Normalization Script drop-down menu. To add additional transparency- or normalization-related changes to a preloaded script, copy the content of the preloaded script and create a new script with the copied content plus additional desired changes.

The following preloaded scripts are provided with Unified CM Release 9.0 and later releases:

- Refer-passthrough—Used to pass through an inbound in-dialog REFER (without Replaces) message to the other side of a call arc, if it is a SIP trunk.The Lua script will copy the Refer-To and Referred-By headers from the inbound REFER message and save them in the transparency object.
- HCS-PCV-PAI-passthrough—This script is used to:
  - Pass through a P-Charging-Vector header for INVITE, UPDATE, and 200 OK
  - Use the configured term-ioi while adding the P-Charging-Vector to 200 OK
  - Pass through a P-Asserted-Identity header for INVITE
- vcs-interop—Used to allow proper interoperation between Unified CM and VCS. This script specifically handles the differences in how the two nodes support SRTP and will change the right side of URIs in the From, Remote-Party-Id and P-Asserted-Id headers to use the configured top-level domain instead of the IP address of Unified CM.
- diversion counter—Used to handle the diversion counter parameter for call forward and diversion scenarios. This script should be attached to both the incoming and outgoing trunks. If there is a call diversion or call forward within the cluster, then this script will adjust the counter parameter in the outgoing diversion header. If there is no call forwarding within the cluster, then this script will simply pass through the counter parameter from the inbound to the outbound side.

The following is a an addition to an existing chapter in the *Developer Guide for SIP Transparency and Normalization*.

Diversion counter

The diversion counter script handles the diversion counter parameter for call forward scenarios. The diversion counter script provides the following functionality:

- Acts as a pass-through diversion counter parameter for a basic tandem (trunk-to-trunk) call with no diversions within the Unified CM cluster.
- Handles the diversion counter parameter for a tandem call with one or more diversions within the Unified CM cluster.
- Handles the diversion counter parameter for a tandem call when the inbound INVITE message has more than two Diversion headers and there is also one or more diversions within the Unified CM cluster.

Exceptions

The diversion counter script has the following exceptions:

- The diversion counter script is applicable only for tandem calls.
- If there are multiple diversions within the cluster, the diversion counter parameter is increased by just one.

Additional information

For complete documentation for the SIP Redirection Counter feature, refer to the *Developer Guide for SIP Transparency and Normalization*.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

SIP normalization and transparency

SIP normalization and transparency allow Cisco Unified Communications Manager to interoperate seamlessly 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 another.

Cisco Unified Communications Manager now supports SIP transparency and normalization for SIP lines. Previously, the feature was available for SIP trunks only.

Cisco Unified Communications Manager Administration considerations

The following changes were made on the **Device** > **Device Settings** > **SIP Normalization Script** menu:

- Script Execution Error Recovery Action—The SIP Reset Trunk/Restart Device menu option was added.
- System Resource Error Recovery Action—The SIP Reset Trunk/Restart Device menu option was added.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

A new set of performance counters has been added under the Cisco SIP Line Normalization heading. The counters themselves are very close to the existing counters for SIP trunks, which can be viewed under Cisco SIP Normalization. However, Performance counters for SIP lines differ in the following manner:

- For SIP lines, each script has one set of performance counters. This is true even if two endpoints share the same script.
- For SIP trunks, each device that has an associated script causes a new instance of these counters to be created.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Single step IP and hostname changes in CUCM cluster

Cisco Unified Communications Manager Administration considerations

Prerequisite checklist

There are a number of prerequisite steps that must be taken prior to changing the hostname:

- Audit your cluster to identify the IP addresses and hostnames of all current nodes.
- Go to the external DNS server and ensure it is ready to be updated. Change the DNS record of the server to point to the new IP addresses you are changing to, and ensure forward (A) and reverse (PTR) records are updated correctly.
- Verify that the network between cluster nodes is working correctly and that the cluster has a valid security password
    - The cluster security password, as well as the network between cluster nodes, can be verified by executing the "show network cluster" CLI command on the Publisher node.
    - When all nodes (other than the Publisher) in the cluster are in the authenticated state, you may conclude that the cluster security passwords are matching and that network connectivity from Publisher to Subscribers is working correctly.
- Verify that the cluster database replication is functioning correctly before moving any servers
    - The Cluster Database Replication status can be verified most quickly by executing "utils dbreplication runtimestate" CLI command on the Publisher node.
    - The column named "Replication Setup (RTMT) & details" indicates what the current database replication status is for a given node. When Database Replication within the cluster is working correctly, the following appears in that column: "(2) Setup Completed".
- Perform a DRS Backup of the cluster.

Note DNS servers comprise part of the external network infrastructure. Unified CM nodes do not and cannot host or provide DNS services.

Note Please verify that the new hostname is unique across the cluster. If DNS Services are utilized, you must complete DNS configuration update(s) with the new hostname before proceeding. To recognize the new hostname, all nodes within the cluster must be manually rebooted. Once the hostname is changed in a virtualized environment, licenses must be rehosted.

There are two methods available for changing the hostname for servers that are defined by a hostname:

- Change hostname via GUI
- Change hostname via Unified Communications Operation System Administration GUI

Change hostname using Unified Communications Operation System Administration GUI

This procedure describes how to use the GUI to change the hostname for a publisher or subscriber server that is defined by a hostname in Unified CM.

Unless otherwise stated, each step in this procedure applies to both publisher and subscriber servers.

Procedure

1. Complete the Prerequisite checklist.
2. To change the host name, the IP address and, if necessary, the default gateway to the new address of the server, perform the following tasks:
   a. Navigate to **Settings > IP > Ethernet**
   b. Change the hostname, IP address and, if necessary, the default gateway to the new address.
   c. Click **Save**, which automatically reboots the server with the new changes.

Note Changing the hostname triggers an automatic, self-signed Certificate Regeneration. If your cluster is using CA-signed certificates, you will need to have them re-signed.

Note If cluster security is in mixed mode, after the server reboots automatically, secure connections to this server fail until you run the CTL client and update the CTL file.

3. Once all changes have been made to all individual servers, a reboot of the entire cluster is required (you do not need to reboot each time). From the Cisco Unified Communications Operating System Administration or CLI , reboot all other servers in the cluster, beginning with the publisher, to update the local name resolutions files, such as hosts/rhosts/sqlhosts/service.

Note Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

4 Verify that the name-IP association that was made in step 2 propagates to other nodes by using the **utils network host** and **show tech network hosts** CLI commands on all cluster nodes:

```
admin:utils network host pub-4
Hostname sub-4 resolves to 198.50.103.11
admin:show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
192.0.2.0 localhost
198.51.100.10 pub-1.cisco.com pub-1
198.51.100.11 tftp-1.cisco.com tftp-1
198.51.100.12 tftp-2.cisco.com tftp-2
198.51.100.10 sub-1.cisco.com sub-1
198.51.100.11 sub-3.cisco.com sub-3
198.50.103.10 sub-2.cisco.com sub-2
198.50.103.11 sub-4.cisco.com sub-4
198.51.100.12 sub-5.cisco.com sub-5
198.51.100.13 sub-7.cisco.com sub-7
198.50.101.12 tftp-3.cisco.com tftp-3
198.51.109.20 cups1.heroes.com cups1
198.50.103.13 sub-6.cisco.com sub-6
admin:
```

Alternatively, you can use the **utils diagnose module validate_network** command on all cluster nodes. This diagnostics module ensures that, if DNS client services are configured, connectivity to DNS server is present, and Forward (A) and Reverse (PTR) records are present and match the server IP address as well as hostname.

Caution Do not proceed if the new hostname does not resolve to the correct IP address.

5 From the publisher node, run **utils dbreplication** reset all to set up replication across the whole cluster again.

Change hostname using Unified Communications Operation System Admin CLI

This procedure describes how to use the CLI command to change the hostname for a publisher or subscriber server that is defined by a hostname in Unified CM.

Unless otherwise stated, each step in this procedure applies to both publisher and subscriber servers.

Procedure

1 Complete the Prerequisite checklist.

2 To change the host name, the IP address and, if necessary, the default gateway to the new address of the server, perform the following tasks:

   a Enter the CLI command **set network hostname** hostname

   b Enter **Yes** and press **Enter**. This action automatically reboots this server with the new hostname.

Note Changing the hostname triggers an automatic, self-signed Certificate Regeneration. If your cluster is using CA-signed certificates, you will need to have them re-signed.

Note If cluster security is in mixed mode, after the server reboots automatically, secure connections to this server fail until you run the CTL client and update the CTL file.

3 Use the **admin:set network ip eth0 ?** CLI command to change the IP address configuration (including the IP address itself), network mask, and default gateway:

```
admin:set network ip eth0 ?
Syntax:
set network ip eth0 addr mask
addr mandatory IP addr to be assigned
mask mandatory IP mask to be assigned
gw mandatory IP default gw to be assigned
admin:help set network ip eth0
ip help:
This will set the ethernet interface eth0 to a new IP address, mask
and default gateway, then cause a restart of the system
Example:
admin:set network ip eth0 192.168.1.5 255.255.255.0 192.168.1.1
*** W A R N I N G ***
This will cause the system to restart - Do you want to continue ?
Enter "yes" to continue and restart or any other key to abort
yes
executing...
Broadcast message from root (Thu Jun 24 13:00:21 2004):
The system is going down for restart NOW!
```

4 Once all changes have been made to all individual servers, a reboot of the entire cluster is required (you do not need to reboot each time).

From the Cisco Unified Communications Operating System Administration or CLI , reboot all other servers in the cluster, beginning with the publisher, to update the local name resolutions files, such as hosts/rhosts/sqlhosts/service.

Note Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

5 Verify that the name-IP association that was made in step 4 propagates to other nodes by using the **utils network host** and **show tech network hosts** CLI commands on all cluster nodes:

```
admin:utils network host pub-4
Hostname sub-4 resolves to 198.50.103.11
admin:show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
192.0.2.0 localhost
198.51.100.10 pub-1.cisco.com pub-1
198.51.100.11 tftp-1.cisco.com tftp-1
198.51.100.12 tftp-2.cisco.com tftp-2
198.51.100.10 sub-1.cisco.com sub-1
198.51.100.11 sub-3.cisco.com sub-3
198.50.103.10 sub-2.cisco.com sub-2
198.50.103.11 sub-4.cisco.com sub-4
198.51.100.12 sub-5.cisco.com sub-5
198.51.100.13 sub-7.cisco.com sub-7
198.50.101.12 tftp-3.cisco.com tftp-3
198.51.109.20 cups1.heroes.com cups1
198.50.103.13 sub-6.cisco.com sub-6
admin:
```

Alternatively, you can use the **utils diagnose module validate_network** command on all cluster nodes. This diagnostics module ensures that, if DNS client services are configured, connectivity to DNS server is present, and Forward (A) and Reverse (PTR) records are present and match the server IP address as well as hostname.

Caution Do not proceed if the new hostname does not resolve to the correct IP address.

6 From the publisher node, run **utils dbreplication reset all** to set up replication across the whole cluster again.

Post-Change Task List

After you finish changing the IP addresses of your cluster, complete the following tasks.

Procedure

1 For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the CTL file. For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide*.

You can find this document at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

2 After you finish updating the CTL file, restart all nodes in the cluster.

3 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

- To check by using RTMT, access Alert Central and check for ServerDown alerts.
- To check by using the CLI on the first node, enter the following command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

4 Check the DB replication status on all Cisco Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.
- To check by using the CLI, enter the command that the following example shows:

```
admin: utils dbreplication runtime
==>query class :
- Perf class (Number of Replicates Created and State of Replication) has instances
 and values:
ReplicateCount -> Number of Replicates Created = 344
ReplicateCount -> Replicate_State = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

  - 0—Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since the subscriber was installed.
  - 1—Replicates have been created, but their count is incorrect.

- 2—Replication is good.
- 3—Replication is bad in the cluster.
- 4—Replication setup did not succeed.

5 In Cisco Unified Reporting, generate the Unified CM Database Status report. Look for any errors or warnings in this report.

6 In Cisco Unified Reporting, generate the Unified CM Cluster Overview report. Look for any errors or warnings in this report.

7 Reconfigure the netdump server and clients by using the **utils netdump** CLI commands. For more information, see Appendix A in the *Cisco Unified Communications Operating System Administration Guide*.

8 Run a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the Disaster Recovery System Administration Guide for your release.

Note You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

9 Update all relevant IP phone URL parameters.

10 In Cisco Unified Communications Manager Administration under **System > Enterprise Parameters**, update all relevant IP phone services.

11 Update IPSec tunnels that terminate to the Cisco Unified Communications Manager.

12 Update RTMT custom alerts and saved profiles:

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure these custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and re-add these counters and then save the profile to update it to the new IP address.

13 Update the DHCP server that runs on Cisco Unified Communications Manager.

14 Check and make any required configuration changes to other associated Cisco Unified Communications components, including the following ones:

Note Consult the documentation for your product to determine how to make any required configuration changes.

- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Express
- SIP/H.323 trunks
- IOS Gatekeepers

- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- DHCP Scopes for IP phones
- SFTP servers that are used for Cisco Unified Communications Manager trace collection, CDR export, or as a DRS backup destination
- IOS hardware resources (conference bridge, media termination point, transcoder, RSVP agent) that register with Cisco Unified Communications Manager
- IPVC video MCUs that register or integrate with Cisco Unified Communications Manager
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- Associated routers and gateways

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

SNMP and billing setup using syslog destination address

The documentation for this feature is provided in the *Cisco Unified Communications Manager XML Developers Guide*.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

URI dialing and Intercluster Lookup Service

Cisco Unified Communications Manager supports dialing using directory URIs for call addressing. Directory URIs look like email addresses and follow the username@host format where the host portion is an IPv4 address or a fully qualified domain name. A directory URI is a uniform resource identifier, a string of characters that can be used to identify a directory number. If that directory number is assigned to a phone then Cisco

Unified Communications Manager can route calls to that phone using the directory URI. URI dialing is available for SIP and SCCP endpoints that support directory URIs.

When the Intercluster Lookup Service (ILS) is configured on multiple Cisco Unified CM clusters, ILS updates Cisco Unified Communications Manager with the current status of remote clusters in the ILS network. ILS runs on a cluster-wide basis. When you configure ILS on one cluster node, ILS propagates those configurations out to the other nodes in the cluster.

The ILS cluster discovery service allows Cisco Unified Communications Manager to learn about remote clusters without the need for an administrator having to manually configure connections between each cluster.

The ILS URI Replication feature enables ILS with the ability to exchange directory URI catalogs with the other clusters in an ILS network. URI Replication provides support for intercluster URI dialing.

Cisco Unified Communications Manager Administration considerations

Service parameter and enterprise parameter changes:

A new enterprise parameter, called Directory URI Alias Partition has been added under End User Parameters. It allows you to alias the default directory URI partition to another partition.

The System menu contains the following updates:

- **System** > **Device Pool**— A new section, called Inbound Call Settings, has been added to the Phone Settings section. The new section contains a new drop-down list box called Calling Party Transformation CSS. Upon receiving a call from any device in this device pool, Cisco Unified Communications Manager applies the transformation pattern to the calling party number.
- **System** > **LDAP Directory**— A Directory URI field has been added to the LDAP Directory Configuration window. This field allows you to import directory URIs for a user from a corporate LDAP directory.

The Call Routing menu contains the following changes:

- **Call Routing** > **SIP Route Pattern**— The SIP Trunk drop-down list box has been renamed to SIP Trunk/Route List. The field allows you to associate the route pattern to a SIP trunk or a route list.
- **Call Routing** > **Directory Number**— The Directory Number Configuration window has the following updates:

  A Directory URIs section has been added with the following fields:

  - Primary— Check this radio button to assign this directory URI as the primary directory URI for this directory number.
  - URI— Enter the directory URI that you want to assign to this directory number.
  - Partition—Enter the partition to which you want to assign this directory URI.
  - Add Row—Click this button to add a new row where you can add a new directory URI. You can associate up to five directory URIs to a single directory number.

  The following fields now support directory URIs:

  - Forward All
  - Forward Busy External
  - Forward Busy Internal
  - Forward No Answer External

- Forward No Answer Internal
- Forward on CTI Failure
- Forward No Coverage External
- Forward No Coverage Internal
- Forward Unregistered External
- Forward Unregistered Internal
- MLPP Alternate Party Settings: Target (Destination)

- **Call Routing** > **Intercluster Directory URI Configuration** > **Intercluster Directory URIs**— A new configuration window has been added with the following fields:
  - Exchange Directory URI Catalogs with Remote Clusters—Check this check box to enable ILS to support intercluster URI dialing.
  - Route String —Enter the route string for your local cluster.
  - Export Local Directory URIs—Check this check box to export local directory URI catalogs to a CSV file.

- **Call Routing** > **Intercluster Directory URI Configuration** > **Intercluster Directory URIs**— A Directory URIs section has been added that contains the following fields:
  - Name—Enter a name for the imported directory URI catalog.
  - Description—Enter a description for the imported directory URI catalog.
  - Route String—Enter the SIP route string for the call control system from which the catalog was imported.

- **Call Routing** > **Intercluster Directory URIs Imported Directory URIs**— A new window has been added that lists imported directory URIs and imported directory URI catalogs.

The Advanced Features menu contains the following changes:

- **Advanced Features > ILS Configuration**—A new configuration window has been added that contains the following fields:
  - Role—Enter a role for the cluster.
  - Register to Another Hub—This button only appears if ILS is configured on the local cluster. Click this button to register this cluster to another hub cluster.
  - Synchronize Clusters Every—Enter a synchronization value for the cluster. All nodes in the cluster synchronize their settings at the end of this interval.
  - Activated—To activate ILS on a cluster node, use the arrows to move the server to the Activated list box and click **Save**.
  - Deactivated—To deactivate ILS on a cluster node, use the arrows to move the server to the Deactivated list box and click **Save**.
  - Registration Server—This text box appears if you activate ILS and click **Save**. Enter the IP address of any server on the hub cluster on which you want to connect.

◦ ILS Clusters and Directory URI Imported Catalogs—This table provides an overview of status of the ILS network.

The Device menu contains the following changes:

- **Device** > **Phone**—A new Call Routing section has been added with an Inbound Calls section and an Outbound Calls section. Cisco Unified Communications Manager applies the Inbound Calls settings as soon as it receives a call from this phone. Cisco Unified Communications Manager applies the Outbound Calls settings just before it forwards a call to the phone. The Inbound Call section contains the following new fields:
  - Calling Party Transformation CSS—From this drop-down list box, choose a Calling Party Transformation CSS to apply to the inbound call settings for the phone.
  - Use Device Pool Calling Party Transformation CSS—Check this check box to apply the Calling Party Transformation CSS that is applied to the device pool.

  The Outbound Calls section has been added, but the fields that are contained in this section are the Calling Party Transformation CSS drop-down list box and Use Device Pool Calling Party Transformation CSS check box that were in previous releases.
- **Device** > **Trunk**—The Calling and Connected Party Info Format drop-down list box has been added. This option allows you to configure whether Cisco Unified Communications Manager includes a directory URI, directory number, or both, in SIP invites for both the calling and connected party.
- **Device** > **Device Settings** > **SIP Profile**—The Dial String Interpretation drop-down list box has been added. In this drop-down list box, you can configure the policy Cisco Unified Communications Manager uses to determine if a dialed number is a directory number or directory URI.

The User Management menu contains the following updates:

- **User Management** > **End User**—The Directory URI field has been added.
- **User Management** > **User/Phone Add** > **End Users**—The Directory URI field has been added.

The Bulk Administration menu has been updated. See Bulk Administration considerations for details.

Bulk Administration considerations

The Bulk Administration Tool, has a number of updates for URI dialing.

A new configuration window has been added under the **Bulk Administration** > **Imported Directory URIs** > **Insert Imported Directory URIs** menu path with the following fields:

- File Name—Choose the CSV file you want to use to insert imported directory URIs.
- Imported Directory URI Catalog—Choose the imported directory URI catalog where you want to insert directory URIs.
- Job Description—Click the radio button that corresponds to when you want to run the job.

The Phones menu that can be accessed by choosing **Bulk Administration** > **Phones** supports directory URIs for the following menu options:

- Create Phone File Format
- Add Phone File Format

- Validate Phones
- Insert Phones
- Update Phones
- Delete Phones
- Export Phones
- Add/UpdateLine

The Users menu that can be accessed by choosing **Bulk Administration** > **Users** supports directory URIs for the following menu options:

- Insert Users
- Update Users

The Phones & Users menu that can be accessed by choosing **Bulk Administration** > **Phones & Users** supports directory URIs for the following menu options:

- Insert Phones with Users
- Validate Phones/Users

The User Device Profiles menu that can be accessed by choosing **Bulk Administration** > **User Device Profiles** supports directory URIs for the following menu options:

- Create UDP File Format
- Add UDP File Format
- Validate UDP
- Insert UDP
- Update UDP
- Delete UDP
- Export UDP
- AddUpdateLines

The Bat.xlt file contains options for inserting columns that support directory URIs. The following tabs in the bat.xlt file support directory URIs:

- Phones—On the Phones tab you can add up to five directory URIs, assign each to a partition, and select the Primary directory URI.
- UserDeviceProfiles—On the UserDeviceProfiles tab you can add up to five directory URIs, assign each to a partition, and select the Primary directory URI.
- AddLines—On the AddLines tab you can add up to five directory URIs, assign each to a partition, and select the Primary directory URI.
- Users—On the Users tab, you can assign a primary directory URI to an end user.

  UpdateUsers—On the UpdateUsers tab, you can update an existing user with a primary directory URI.

Throughout the user interface and the bat.xlt spreadsheet, the following fields now support directory URIs. Previously, these fields supported directory numbers only:

- Forward All Destination
- Forward Busy Destination External
- Forward Busy Destination Internal
- Forward No Answer Destination External
- Forward No Answer Destination Internal
- Forward No Coverage Destination External
- Forward No Coverage Destination Internal
- Forward on CTI Failure Destination
- Speed Dial
- BLF Speed Dial

CDR/CAR considerations

The following CDR fields were added for URI Dialing:

- callingPartyNumber_uri
- originalCalledPartyNumber_uri
- finalCalledPartyNumber_uri
- lastRedirectDn_uri

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

The Dialed Number Analyzer now supports troubleshooting using directory URIs.

Two new reports have been added to Cisco Unified Reporting:

- Duplicate Directory URIs—Provides a list of duplicated directory URIs on the system.
- Unified CM Users Sharing Primary Extensions—Provides a list of users that share a primary extension on the system.

Additional information for URI dialing

Directory URI format

Directory URIs are alphanumeric strings consisting of a user and a host address separated by the @ symbol. Cisco Unified Communications Manager supports the following formats for directory URIs:

- user@domain (for example, joe@cisco.com)
- user@ip_address (for example, joe@10.10.10.1)

Cisco Unified Communications Manager supports the following formats in the user portion of a directory URI (the portion before the @ symbol):

- Accepted characters are a-z, A-Z, 0-9, !, $, %, &, *, _, +, ~, -, =, \, ?, \, ‘, ,, ., /.
- The user portion has a maximum length of 47 characters.
- The user portion accepts percent encoding from %2[0-9A-F] through %7[0-9A-F]. For some accepted characters, Unified CM automatically applies percent encoding. See below for more information on percent encoding.
- The user portion is case sensitive.

Cisco Unified Communications Manager supports the following formats in the host portion of a directory URI (the portion after the @ symbol):

- Supports IPv4 addresses or fully qualified domain names.
- Accepted characters are a-z, A-Z ,0-9, hyphens, and dots.
- The host portion cannot start or end with a hyphen.
- The host portion cannot have two dots in a row.
- Minimum of two characters.
- The host portion is not case sensitive.

Due to database restrictions, the Directory URI field has a maximum length of 254 characters.

Note You can also enter a directory number in the user portion of a directory URI. However, Cisco Unified Communications Manager may treat the directory URI as a directory number depending on which Dial String Interpretation option you choose for the SIP Profile.

Note For compatibility with third-party call control systems, we recommend using lower case for directory URIs.

Percent encoding of directory URIs

In the user portion of a directory URI, Unified CM automatically applies percent encoding to the following characters when the directory URI is saved in the database:

% ^ ` { } | \ : ” < > [ ] \ ‘ and spaces

When percent encoding is applied, the digit length of the directory URI increases. For example, if you input joe smith#@cisco.com (20 characters) as a directory URI, Cisco Unified Communications Manager stores the directory URI in the database as joe%20smith%23@cisco.com (24 characters). Due to database restrictions, Cisco Unified Communications Manager rejects any attempt to save a directory URI of greater than 254 characters.

Directory URI format exception for Bulk Administration

Within Cisco Unified CM Administration, you can enter directory URIs with embedded double quotes or commas. However, when you use Bulk Administration to import a CSV file that contains directory URIs with embedded double quotes and commas, you must use enclose the entire directory URI in double quotes and escape the embedded double quotes with a double quote. For example, the Jared, "Jerry",Smith@test.com directory URI must be input as "Jared,""Jerry"",Smith@test.com" in the CSV file.

Directory URI provisioning

In Cisco Unified CM Administration, you can assign directory URIs in the local cluster in the following ways:

- End User Configuration—In End User Configuration, you can create end users and assign a phone, primary extension, and directory URI to that end user. Alternatively, If you synchronize your corporate LDAP directory with Cisco Unified Communications Manager, the LDAP data automatically populates for your end users. If the users in your LDAP directory have a phone, primary extension, and directory URI, they will automatically have directory URIs in Cisco Unified Communications Manager End User Configuration after the LDAP synchronization.
- Directory Number Configuration—In Directory Number Configuration, you can configure a directory number and associate a directory URI to that directory number. If that directory number is assigned to a phone, Cisco Unified Communications Manager allows you to dial that phone using the directory URI.

For both end user configuration and directory number configuration, you can also use Bulk Administration to import end users, directory URIs, directory numbers, and phones into Cisco Unified Communications Manager by bulk. See the *Cisco Unified Communications Manager Bulk Administration Guide* for more information.

For intracluster URI dialing, you must assign your directory URIs to a partition and calling search space. See Set up URI dialing for more information.

For intercluster URI dialing, Cisco Unified Communications Manager uses the Intercluster Lookup Service (ILS) to replicate directory URIs to other clusters in the ILS network. If ILS is configured to support intercluster directory URI Replication, each cluster sends out its catalog of known directory URIs to the other clusters in the ILS network. See Directory URI Replication with ILS for more information.

Directory URI and directory number dial string interpretation

Each phone that registers with Cisco Unified Communications Manager registers to its directory number. If a directory URI is associated with that directory number, users can dial that phone using the directory number or the directory URI—either will reach the same destination. However, because directory numbers and directory

URIs are saved in different lookup tables in the database, Cisco Unified Communications Manager must be able to determine which dialing format is used, or it will not be able to route the call.

The Dial String Interpretation field that appears in the SIP Profile Configuration window allows you to set the rules that Cisco Unified Communications Manager uses to examine the user portion of a dial string and determine whether to route the call as a directory URI or a directory number. Because directory URIs can use both alpha and numeric characters, many dial strings are arbitrary and could be configured as either a directory URI or directory number. For example, you can configure Cisco Unified Communications Manager to route a dial string of 1234ABCD@10.10.10.1 as a directory number or as a directory URI. To ensure that calls are not dropped, you must configure a consistent policy for your network.

For more information on the Dial String Interpretation field, see the SIP Profile settings section in the *Cisco Unified Communications Manager Administration Guide*.

Directory URI call routing

Unified CM uses the following logic to route calls that are placed to a directory URI:

- Unified CM checks if the dial string is for a directory number. If the dial string is a directory number, Cisco Unified CM routes the call as a directory number.
- Else, Unified CM checks local calling search spaces and the local directory URI lookup table to see if the directory URI is in the local cluster. If the directory URI is on cluster, Cisco Unified CM routes the call to the appropriate endpoint.
- Else, Unified CM checks the URI catalogs that ILS maintains. If the directory URI is in a URI catalog, Cisco Unified CM finds the route string for the URI catalog and tries to match it to a SIP route pattern. If a matching SIP route pattern is found, Cisco Unified CM routes the call to the trunk that is associated with that route pattern.
- Else, Unified CM tries to match the host portion of the directory URI to a SIP route pattern. If the host portion matches a SIP route pattern, Cisco Unified CM routes the call to the SIP trunk that is associated to that route pattern.
- Else, Unified CM blocks the call.

Directory URI interoperability with VCS or third party system

Cisco Unified Communications Manager gives users with a supported endpoint the ability to place calls to alphanumeric URIs such as johnsmith@acme.com. The simplest way to route directory URI calls from a supported endpoint on Cisco Unified Communications Manager to an endpoint on a Cisco TelePresence Video Communications Server (VCS) or a third party call control system is to configure a domain-based SIP route pattern. For example, you can configure a SIP route pattern of acme.com to route calls addressed to the acme.com domain out a SIP trunk that is configured for the Cisco TelePresence VCS or a third party call control system.

In situations where you have more than one Cisco TelePresence VCS or third party call control systems that use the same domain name, Cisco Unified Communications Manager can use the Intercluster Lookup Service (ILS) to provide URI dialing interoperability. For each Cisco TelePresence VCS, or third party system, you must manually create a csv file with the directory URIs that are registered to that call control system.

On a Cisco Unified Communications Manager cluster that is set up as a hub cluster in an ILS network, you can create an Imported directory URI catalog for each Cisco TelePresence VCS, or third party system, and assign a unique route string for each catalog. After you import the csv files into their corresponding Imported

directory URI catalog, ILS replicates the imported directory URI catalog and route string to the other clusters in the ILS network.

On each Cisco Unified Communications Manager cluster, configure SIP Route Patterns that match the route string assigned to each Imported directory URI catalog in order to allow Cisco Unified Communications Manager to route directory URIs to an outbound trunk that is destined for the Cisco TelePresence VCS or third party system.

For more information on how to import directory URIs from a VCS into Cisco Unified Communications Manager, see the "Import directory URIs from a non-ILS system" procedure in the Intercluster Directory URI chapter of the *Cisco Unified Communications Manager Administration Guide*.

Cisco Unified Communications Manager also provides directory URI export functionality. You can export all directory URIs that were configured in the local cluster, including those that were imported from an LDAP directory, to a csv file that you can import into the other call control system. For more information on how to export directory URIs from Cisco Unified Communications Manager to a csv file, see the "Intercluster directory URI settings" section in the Intercluster Directory URI chapter of the *Cisco Unified Communications Manager Administration Guide*.

Related Topics

Import Directory URIs from a non-ILS system, on page 145
Intercluster directory URI settings

Directory URI LDAP integration

Cisco Unified Communications Manager supports synchronization of directory URI fields in Cisco Unified CM Administration with data from a corporate LDAP directory.

When you synchronize with an LDAP directory, Unified CM automatically assigns the directory URI value that you choose from the LDAP directory as the primary directory URI for that end user. Even if you have already configured a directory URI as the primary directory URI for that end user's primary extension, the LDAP value overrides the value that is configured in Cisco Unified CM Administration

Note The user portion of a directory URI is case sensitive. As a result, whatever case the directory URI has in the LDAP directory is the case in Cisco Unified Communications Manager. For example, if the directory URI value in LDAP is JOE@cisco.com, calls to joe@cisco.com in Cisco Unified Communications Manager will fail.

Note For compatibility with third party call control systems, Cisco recommends using lower case for directory URIs.

Note For Cisco Unified Communications Manager systems where LDAP synchronization was configured prior to Release 9.0, the directory URI field is not automatically enabled for synchronization. You must create a new LDAP synchronization agreement.

Directory URI and directory number blended address

Cisco Unified Communications Manager supports blended addressing of directory URIs and directory numbers. When blended addressing is enabled across the network, Cisco Unified Communications Manager inserts both the directory URI and the directory number of the sending party in outgoing SIP Invites, or responses to SIP Invites. The destination endpoint has the option of using either the directory URI or the directory number for its response—both will reach the same destination.

Cisco Unified Communications Manager uses the x-cisco-number tag in the SIP identity headers to communicate a blended address. When both a directory URI and directory number are available for the sending phone and blended addressing is enabled, Cisco Unified Communications Manager uses the directory URI in the From fields of the SIP message and adds the x-cisco-number tag with the accompanying directory number to the SIP identity headers. The x-cisco-number tag identifies the directory number that is associated with the directory URI.

For Cisco Unified Communications Manager to deliver a SIP message with blended addressing, the following conditions must be true:

- For all SIP trunks between the phones, the Calling and Connected Party Info Format drop-down list box must be set to **Deliver URI and DN in connected party**.
- Both a directory URI and a directory number must be configured for the phone that is sending the SIP message.
- The destination endpoint must support blended addressing.

For SIP trunks, blended addressing is enabled in the Trunk Configuration window of Cisco Unified CM Administration by setting the Calling and Connected Party Info Format drop-down list box to **Deliver URI and DN in connected party**. When Cisco Unified Communications Manager receives a SIP message with a blended address that is to be forwarded out a trunk, Cisco Unified Communications Manager checks whether blended addressing is enabled on the trunk before forwarding the message. If blended addressing is not enabled on the trunk, Cisco Unified Communications Manager removes the x-cisco-number tag before forwarding the SIP message.

For SIP lines, blended addressing is enabled by default. However, if a SIP message with a blended address is being forwarded out a SIP line to the destination endpoint, Cisco Unified Communications Manager checks whether the endpoint supports blended addressing. If the destination endpoint does not support blended addressing, Cisco Unified Communications Manager removes the x-cisco-number tag before forwarding the SIP message to the endpoint.

Blended addressing can be applied to the RPID, PAI, PPI, and Diversion headers.

Example 1

Bob at Cisco makes a call from extension 2100. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to **Deliver DN only in connected party**. Blended addressing is not applied and the x-cisco-number tag is not added to the outgoing SIP message.

```
From:<sip:2100@10.10.10.1>
Remote-Party-ID:<sip:2100@10.10.10.1>;party=calling
```

Example 2

Jill at Cisco makes a call from extension 2030. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to **Deliver URI only in connected party**. Blended addressing is not applied and the x-cisco-number tag is not added to the outgoing SIP message.

```
From:<sip:jill@cisco.com>
Remote-Party-ID:<sip:jill@cisco.com>;party=calling
```

Example 3

Alice at Cisco makes a call from extension 2000. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to **Deliver DN and URI in connected party**. Blended addressing is applied. Cisco Unified Communications Manager adds the x-cisco-number tag to the SIP identity header.

```
From:<sip:alice@cisco.com>
Remote-Party-ID:<sip:alice@cisco.com;x-cisco-number=2000>;party=calling
```

John at Cisco extension 4003 receives Alice's call, but John has his office phone set to forward calls to his home phone. If blended addressing is enabled, Cisco Unified Communications Manager adds a Diversion header with the x-cisco-number tag, and forwards the SIP INVITE to John's home phone.

```
From:<sip:alice@cisco.com>
Diversion: <sip:john@cisco.com;x-cisco.number=4003>reason=no-answer
Remote-Party-ID:<sip:alice@cisco.com;x-cisco-number=2000>;party=calling
```

Directory URI Replication with ILS

Cisco Unified Communications Manager uses the Intercluster Lookup Service (ILS) to support intercluster URI dialing. Using ILS, you can create large networks of remote Cisco Unified Communications Manager clusters. ILS also contains an optional directory URI replication feature that allows the clusters in an ILS network to replicate their directory URIs to the other clusters in the ILS network.

Directory URI Replication is configured individually for each cluster. Be aware that if you leave the feature disabled on a single cluster, it can affect other clusters in the network. For example, if directory URI replication is configured across the ILS network but is left disabled on a single hub cluster, the spoke clusters that are connected to that hub cannot exchange directory URIs with the rest of the ILS network.

To enable URI Replication in a cluster, check the Exchange Directory URIs with Remote Clusters check box that appears in Intercluster Directory URI Configuration. When this check box is checked, each cluster sends the following to the other clusters in the ILS network:

- All directory URIs known by the local cluster.
- The local route string for each set of directory URIs.

Directory URI catalog types

Within an individual cluster, directory URIs can be categorized as follows:

- Local directory URIs—Directory URIs that are configured on the local system and which are saved in the local Unified CM database.
- Remote directory URIs—Directory URIs that were configured in another cluster and then replicated to this cluster.
- Imported Directory URI catalogs—Third party directory URIs that were manually imported into this cluster.

- Remote Imported Directory URI catalogs—Third party directory URIs that were manually imported into another cluster in the ILS network and then replicated to this cluster with ILS.

Local directory URIs are saved in the local Unified CM database. All other directory URIs are saved in CSV files that are maintained by ILS. When directory URI replication is enabled, ILS exchanges all types of directory URIs to the other clusters in the ILS network.

Route strings

In order to implement intercluster URI dialing, each cluster in the ILS network must be configured with a route string and SIP route patterns that match the route strings to an outbound trunk.

In many cases, the host portion of the directory URI is not granular enough for Unified CM to locate the cluster with the phone that is associated to that directory URI. Route strings provide additional information that Unified CM can use to route a call. When URI Replication is enabled, Unified CM exchanges directory URIs and the route string for the local cluster where that directory URI is saved.

You can create whatever route strings you want. For example, if you are joining clusters in San Jose and Paris, you could assign SanJose.USA.NorthAmerica and Paris.France.Europe as route strings for the two clusters.

After you assign route strings for the various clusters, you must configure SIP route patterns that match the route strings for the next hop clusters in your ILS network. For example, in the San Jose cluster, you could configure a SIP route pattern that routes calls with a route string of Paris.France.Europe to an outbound SIP trunk.

If the San Jose cluster receives a call that is addressed to a directory URI from the Paris cluster, Unified CM checks the list of directory URIs maintained by ILS and pulls the directory URI and its local route string of Paris.France.Europe. If a SIP route pattern is configured that routes calls for Paris.France.Europe, Unified CM sends the call to the outbound trunk for that route pattern.

For more detail on configuring route strings, refer to the Cisco Unified Communications System SRND

ILS cluster discovery

Cluster discovery is the base service that ILS provides. ILS cluster discovery allows Unified CM clusters to learn dynamically about remote Unified CM clusters without the need for an administrator to manually configure connections between those clusters.

For example, if you have an existing ILS network of four Unified CM clusters and you want to add an additional cluster, you can configure ILS on the new cluster and then register that cluster to any hub cluster in the existing ILS network. ILS automatically informs the new cluster of all clusters in the existing network.

Each cluster in an ILS network exchanges update messages, called peer info vectors, that are designed to inform remote clusters of the status of each cluster in the network. The update messages contain information about the known clusters in the network, including:

- Cluster IDs
- Cluster descriptions and versions
- Fully qualified domain name of the host
- IP addresses and hostnames for the cluster nodes that have ILS activated

The ILS cluster discovery feature automatically populates the list of remote clusters that can be viewed in Cisco Unified CM Administration by choosing **Advanced Features > Cluster View**. From this window, you can configure services such as Extension Mobility Cross Cluster, TFTP, and RSVP Agent for remote clusters.

If URI Replication is also enabled in the network, ILS sends separate messages containing the list of directory URIs.

ILS network components

In Cisco Unified CM Administration, you can configure ILS on a pair of clusters and then join those clusters to form an ILS network. ILS allows you to join additional clusters to the network without having to configure the connections between each cluster.

An ILS network comprises the following components:

- Hub clusters
- Spoke clusters
- Directory URI imported catalogs

You must configure each cluster in your ILS network as either a hub cluster or a spoke cluster. Each ILS network must have at least one hub cluster.

You can view the current structure and status of the ILS network from the ILS Clusters and Directory URI Imported Catalogs view in the ILS Configuration window of Cisco Unified CM Administration.

Hub clusters

Each ILS network must have at least one hub cluster. Hub clusters form the backbone of an ILS network. Hub clusters exchange ILS updates with the other hub clusters in the ILS network, and then relay that information to and from their spoke clusters.

ILS uses automesh functionality to create a full mesh connection between all hub clusters within an ILS network. When a new hub cluster registers to another hub cluster in an existing ILS network, ILS automatically creates a full mesh connection between the new hub cluster and all the existing hub clusters in the ILS network.

You can connect a hub cluster to multiple other hub clusters, or you might configure a hub cluster as the only hub cluster in the network. In addition, you can connect a hub cluster to multiple spoke clusters, or you might configure the hub cluster with no spokes clusters.

Spoke clusters

A spoke cluster in an ILS network relies on the hub cluster that it is connected to in order to relay ILS updates to and from the rest of the ILS network. Although a hub cluster can have many spokes, a spoke cluster can have only one hub cluster. Spoke clusters contact only their local hub cluster and never directly contact other hub clusters or other spoke clusters.

Directory URI imported catalogs

You cannot connect a third party call control system into an ILS network. However, in order to provide URI dialing compatibility with third party systems, you can manually import a third party directory URI catalog from a CSV file into any hub cluster in the ILS network. ILS maintains the directory URI imported catalog and replicates that catalog out to the other clusters in the network so that you can dial one of the third party directory URIs from any server in the ILS network. The directory URI imported catalog appears as its own item in the ILS Clusters and Directory URI Imported Catalogs view in the ILS Configuration window.

You can import a third party directory URI catalog into a hub cluster only. You cannot import a third party directory URI catalog into a spoke cluster.

Synchronization updates

For cluster synchronization updates, ILS uses a pull-based model in which an ILS cluster sends out an update request to a remote cluster and the remote cluster responds with the requested information. The time interval between update requests depends on the synchronization interval that is configured in the ILS Configuration window in Cisco Unified CM Administration.

In addition, within an individual ILS cluster, synchronization intervals determine how long it takes for the various cluster nodes to synchronize their ILS settings.

For detailed information on setting up an ILS network topology, see the Cisco Unified Communications System SRND.

Procedures

Set up URI dialing

The following procedure describes how to set up URI dialing in your network.

Procedure

Step 1 Assign directory numbers for the phones in your network.

Step 2 Assign directory URIs to the directory numbers in your network.

Step 3 Assign the partition where you saved your directory URIs to a calling search space.

Step 4 Configure a Dial String Interpretation policy for the SIP profiles in your network.

Step 5 Check the Use Fully Qualified Domain Name in SIP Requests check box for the SIP profiles in your network.

Step 6 For all the SIP trunks in your network, configure the Calling and Connected Party Info Format field.

Step 7 Set up ILS on all clusters in your network.

Step 8 Enable intercluster URI dialing with ILS by checking the Exchange Directory URI Catalogs with Remote Clusters check box in the Intercluster Directory URI Configuration window.

Step 9 In the Intercluster Directory URI Configuration window, enter a route string that remote clusters will use to route to this cluster.

Step 10 Configure SIP route patterns that route to the route strings for the next hop clusters in your ILS network.

Step 11 Associate the SIP route patterns that you created to a SIP trunk or route list.

Step 12 If you are connecting your ILS network to a call control system that is not running ILS, import directory URI catalogs from the other system into Cisco Unified Communications Manager.

Step 13 If your deployment uses digit transformations to transform calling party directory numbers, configure calling party transformation patterns and apply them to the Inbound Call Settings for the phone or device pool. This configuration is required for intercluster calls.

Step 14 If you applied digit transformation patterns in the previous step, configure calling party transformation patterns for the Outbound Call Settings for the phone or device pool. This configuration is required for intracluster calls.

Set up ILS network

The following procedure describes the high-level steps required to configure an ILS network.

Procedure

Step 1 Study your network and design an ILS topology.

Step 2 Assign unique cluster IDs for each cluster in your network.

Step 3 If you want to use TLS authentication between clusters, you must exchange Tomcat certificates between each node in every cluster in the ILS topology. From Cisco Unified Operating System Administration, use the Bulk Certificate Management feature to:

- From each cluster in your network, export certificates to a central location.
- From one server in your ILS network, consolidate exported certificates.
- From each cluster in your network, import certificates into the local cluster.

Step 4 If you want to use TCP password authentication between remote clusters, assign a password for all communications between clusters in your ILS network.

Step 5 Activate ILS on the first hub cluster in your ILS network.

- In Cisco Unified CM Administration, choose **Advanced Features** > **ILS Configuration**.
- Change the Role to **Hub Cluster** and click **Save**.
- In the ILS Configuration Registration popup window, leave the Registration Server text box empty and click **OK**.

Step 6 Activate ILS on the remaining hub and spoke clusters in your ILS network. When prompted for a registration server, enter the IP address of any node that is located in an existing hub cluster in your ILS network and that has ILS activated on the local server.

Step 7 Confirm that your ILS network is configured by viewing the network in the ILS Clusters and Directory URI Imported Catalogs view in the ILS Configuration window. When the full network appears, your ILS network is configured for cluster discovery.

Note The remaining steps are performed only if you want to configure ILS to support intercluster URI dialing.

Step 8 If you want to use ILS to support intercluster URI dialing, check the **Exchange Directory URI Catalogs with Remote Clusters** check box in the Intercluster Directory URI Configuration window.

Step 9 In the Intercluster Directory URI Configuration window, enter a route string for the local cluster.

Step 10 Configure SIP route patterns that match the route strings for your remote clusters to an outbound trunk.

Step 11 If you want to connect your ILS network to a call control system that is not running ILS, such as a Cisco VCS, import directory URI catalogs from the other system into Cisco Unified Communications Manager.

Set up digit transformations for URI dialing

If your network applies digit transformation patterns to calling party directory numbers and you are implementing URI dialing across clusters, you can apply calling party transformation patterns against the Inbound Call Settings of the phone or device pool. This is required because Cisco Unified Communications Manager cannot perform calling party transformations if the calling party transformation is applied based on the called party directory number or pattern.

For intercluster calls, you can apply a digit transformation pattern against a Calling Search Space (CSS) and apply that CSS transformation to the Inbound Call Settings for the phone or device pool. Before routing the call, whether the dialed number is a directory URI or a directory number, Cisco Unified Communications Manager applies the transformation pattern to the calling directory number.

For intracluster calls, if you don't want the calling party transformation to be applied for calls that remain in the local cluster, you can also apply a CSS transformation pattern that strips the digits that were added by the Inbound Call Settings and apply that pattern to the Outbound Call Settings for the phone or device pool. For the device pool, the Calling Party Transformation CSS for outbound calls appears under Device Mobility Related Information.

To apply calling party digit transformations when URI dialing is implemented, do the following:

Procedure

Step 1 In Cisco Unified CM Administration, choose**Call Routing** > **Class of Control** > **Partition** and create a new partition (for example, Change Calling Party XXXX to 8XXXXXXX).

Step 2 Choose**Call Routing** > **Class of Control** > **Calling Search Space** and do the following:

- Create a calling search space (for example, Change Calling Party XXX to 8XXXXXXX).
- In the Available Partitions list box, add the newly created partition (for example, Change Calling Party XXXX to 8XXXXXXX).

Step 3 In Cisco Unified CM Administration, choose **Call Routing** > **Transformation** > **Transformation Pattern** > **Calling Party Transformation Pattern**.

- Create a transformation pattern (for example, XXXX)
- Set the partition to the partition that you created in the previous steps (for example Change Calling Party XXXX to 8XXXXXXX).
- Set the Calling Party Transformation Mask to the desired mask (for example, 8265XXXX).

Step 4 In Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition** and create a new partition (for example, Change Calling Party 8XXXXXXX to XXXX).

Step 5 Choose**Call Routing** > **Class of Control** > **Calling Search Space** and do the following:

- Create a calling search space (for example, Change Calling Party 8XXXXXXX to XXXX).
- In the Available Partitions list box, add the newly created partition (for example, Change Calling Party 8XXXXXXX to XXXX).

Step 6 In Cisco Unified CM Administration, choose **Call Routing** > **Transformation** > **Transformation Pattern** > **Calling Party Transformation Pattern**.

- Create a transformation pattern (for example, 8265XXXX)
- Set the partition to the partition that you created in the previous steps (for example, Change Calling Party 8XXXXXXX to XXXX).
- Set the Calling Party Transformation Mask to the desired mask (for example, XXXX).

Step 7 To assign your transformation patterns to an individual phone, choose **Device** > **Phone** and apply the following settings to the phone:

- For patterns that apply to inbound settings, choose the CSS that contains the pattern from the Calling Party Transformation CSS drop-down list box that appears under Inbound Calls.
- For patterns that apply to outbound settings, choose the CSS that contains the pattern from the Calling Party Transformation CSS drop-down list box that appears under Outbound Calls.

Step 8 Click **Save**.

Note You can also apply the digit transformation patterns to a device pool by choosing**System** > **Device Pool** from Cisco Unified CM Administration. For device pool configuration, the Calling Party Transformation CSS for outbound calls appears under Device Mobility Related Information.

Import Directory URIs from a non-ILS system

Follow this procedure if you are running the Intercluster Lookup Service (ILS) on your local cluster and you want to import directory URIs from a CSV file for a call control system that is not running ILS, such as a Cisco TelePresence Video Communication Server (VCS), or a third-party call control system.

To perform this procedure, the Cisco Bulk Provisioning Service must be running on the local cluster, which must be configured as a hub cluster in an ILS network. After you import the catalog into Cisco Unified Communications Manager, ILS replicates the imported catalog to the other clusters in the ILS network.

Note Within Cisco Unified CM Administration, you can enter directory URIs with embedded double quotes or commas. However, when you use Bulk Administration to import a CSV file that contains directory URIs with embedded double quotes and commas, you must use enclose the entire directory URI in double quotes and escape the embedded double quotes with a double quote. For example, a directory URI of Jared,"Jerry",Smith@test.com must be input as "Jared,""Jerry"",Smith@test.com" in the CSV file.

Procedure

Step 1 In Cisco Unified CM, choose **Routing** > **Directory URIs** > **Imported Directory URI Catalogs**.
Step 2 In the Name field, enter a name for the directory URI catalog.
Step 3 In the Description field, enter a description of the directory URI catalog.
Step 4 In the Route String field, create a route string for the system from which you are importing the URI catalog.
Step 5 Click **Save**.
Step 6 In Cisco Unified CM Administration, choose**Bulk Administration** > **Upload/Download Files**.
Step 7 Click **Add New**.
Step 8 Click **Browse** and select the CSV file for the directory URI catalog that you want to import.
Step 9 In the Select the Target drop-down list box, choose **Imported Directory URIs**.
Step 10 In the Select TransactionType drop-down list box, choose **Insert Imported Directory URIs**.
Step 11 Click **Save**.
Step 12 In Cisco Unified CM Administration, choose **Bulk Administration** > **Imported Directory URIs** > **Insert Imported Directory URIs**.
Step 13 In the File Name drop-down list box, choose the CSV file that contains the imported directory URI catalog.
Step 14 In the Imported Directory URI Catalog drop-down list box, choose the directory URI catalog that you named in the Imported Directory URI Catalog window.
Step 15 In the Job Description text box, enter a name for the job that you are about to run.
Step 16 Select when you want to run the job.

- If you want to run the job now, click the **Run Immediately** radio button, and click **Submit.**
- If you want to schedule the job to run at a specified time, check the **Run Later** radio button and click **Submit**. If you choose this option, you must use the Bulk Administration Job Scheduler to schedule when the job runs.

CLI changes

utils ils findroutestring

This command returns all route strings that are associated with this directory URI, including the route string for the local cluster.

utils ils findroutestring *Directory URI*

Syntax Description

Parameters	Description
Directory URI	Specifies a directory URI address that can be dialed in an outgoing call.

Command Modes Administrator (admin:)

Usage Guidelines This command can be used to troubleshoot problems involving duplicate directory URIs.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM

utils ils findxnode

This command returns the current xnode for the local cluster.

utils ils findxnode

Command Modes Administrator (admin:)

Usage Guidelines This command can be used for troubleshooting ILS communications with remote clusters. The xnode is the server within the cluster that communicates ILS updates with remote clusters. Once you know the xnode, you can run diagnostic traces on the xnode.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM

utils ils lookup

This command returns the route string that is used for call routing when this directory URI is dialed from this cluster.

utils ilslookup *Directory URI*

Syntax Description

Parameters	Description
Directory URI	Specifies a directory URI that can be dialed in an outgoing call

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM

utils ils showpeerinfo

This command returns the peer info vector for either a single cluster in an ILS network, or for all the clusters in an ILS network.

utils ils showpeerinfo *clustername*

Syntax Description

Parameters	Description
clustername	Specifies the fully qualified domain name of the publisher node for a Cisco Unified CM cluster in an ILS network.

Command Modes Administrator (admin:)

Usage Guidelines The peer info vector contains information about a cluster in an ILS network. The available information includes clustername, cluster ID and IP addresses for the cluster nodes. If you want information about a specific cluster in an ILS network, enter the clustername parameter. If you want information on all the clusters in the network, leave the clustername parameter empty

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified CM

User Options page enhancements

Cisco Unified CM User Options has been updated with a new user interface that is aimed at phone users with a single phone and line. The new design provides users with a task-based interface rather than the device-based interface that was used in past releases.

With the new interface, users can configure phone options such as do not disturb, speed dials and ring settings for their Cisco Unified IP phones. The new user options settings are available in the following menus:

- Home—Users can set up alternate numbers, call forwarding, and speed dials for their phones.

- Contacts—Users can build a personal address book with common contacts.
- Directory—Users can access their corporate directory.
- Line Settings—Users can set up options such as voicemail notifications and ring settings for their phone line.
- Phone Settings—Users can set up phone settings such as phone description and language.
- Services—Users can set up phone services for their IP phones.

For detailed procedures, refer to the *Cisco Unified CM User Options Guide*.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

Video for SNR call

In Unified CM, if two endpoints including the remote destination are video capable, then mobility allows video streaming along with audio. The following example demonstrates this scenario:

1. Phone A (video capable) and Phone B are in cluster 1.
2. Phone C (video capable) is the remote destination shared line with Phone B is in cluster 2.

3 Phone A calls Phone B.

4 Phone C rings because of Single Number Reach.

5 If you pick up Phone C and both Phone A and Phone C are video capable, then a video call takes place.

Limitations and Conditions

- If in the entire call setup, Unified CM allocates a software MTP, video streaming is not supported because MTP does not support video streaming.
- A hardware multimedia IOS MTP allocated in the call may result in video with certain conditions:

  If the MTP is allocated because of MTP Required check on trunks and gateways, then video streaming does not occur.

  If Unified Mobility requires MTP for DTMF detection, video is not available.

  If MTP is allocated due to transcoders and a TRP check on devices, trunks, and gateways, video is available.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

Procedures

CLI changes

Video over Wi-Fi

With a dual mode smart client running on a video-capable smart phone and registered to Unified CM, a video call can take place between the smart phone and another video-capable endpoint over VoIP.

If a Cisco Dual Mode for iPhone (TCT) is video capable, it can call another video capable end point through the Unified CM over IP.

A video enable/disable toggle option is available on the device page of Unified CM Administration. Additionally, mid-call features like Hold/Resume, conference, and transfer with video are available.

MTP interactions and Limitations:

- A software MTP allocated in the call does not support video streaming.
- A hardware multimedia MTP allocated allows video, with the condition that MTP allocated due to transcoders, TRP check on devices/trunks/gateways, video is not supported.
- When Unified Mobility requires the MTP for DTMF detection, video is available.
- MTP allocated due to transcoders, TRP check on devices/trunks/gateways, video will be available.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

XML Axis framework 2.0 update

For Cisco Unified Communications Manager 9.0 and later, Serviceability XML APIs provide remote procedure call (RPC) as well as doc/literal style operations for clients. The Serviceability XML is now available on the following servers:

- AXIS 1.4 SOAP server with AXIS-2250 patch
- AXIS 2.0 SOAP server

Complete documentation for this feature is provided in the *Cisco Unified Communications Manager XML Developers Guide*.

Cisco Unified Communications Manager Administration considerations

No changes.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

2000 character LDAP filter size

The documentation for this feature is provided in the Cisco Unified Communications Manager Administration Guide.

Cisco Unified Communications Manager Administration considerations

LDAP Filter Configuration Settings

In Cisco Unified Communications Manager Administration, use the **System** > **LDAP Systen** > **LDAP Custom Filter** menu path to configure LDAP filters.

In the LDAP Filter Configuration window, you specify information about the LDAP filter.

Configuration Settings Table

The following table details the LDAP filter configuration settings.

Table 13: LDAP Custom Filter Settings

Field	Description
LDAP Custom Filter Information	
Filter Name	Enter a name for the LDAP filter. The name can contain a maximum of 64 UTF-8 characters.
Filter	Enter a filter. The filter can contain a maximum of 2048 UTF-8 characters. Enclose the filter text within parentheses (). The LDAP filter filters the results of LDAP searches. LDAP users that match the filter get imported into the Cisco Unified Communications Manager database, while LDAP users that do not match the filter do not get imported. The filter text that you enter must comply with the regular LDAP search filter standards specified in RFC 4515. It is recommended that you verify the LDAP search filter against the LDAP directory/searchbase by using the **ldapsearch** command. You apply LDAP filters to LDAP directories. You can apply an LDAP filter to multiple LDAP directories, and to all LDAP directory types for which the filter is valid.

Bulk Administration considerations

No changes.

CDR/CAR considerations

No changes.

IP phones considerations

No changes.

RTMT considerations

No changes.

Security considerations

No changes.

Serviceability considerations

No changes.

CLI changes

No changes.

CHAPTER 4

Cisco Unified IP Phones

The following table contains the firmware versions for the Cisco Unified IP Phones for Cisco Unified Communications Manager Release 9.0.

Phone family	Release number
Cisco Unified IP Phone 6900 Series	9.3(1)
Cisco Unified IP Phone 7900 Series	9.3(1)
Cisco Unified IP Phone 8941 and 8945	9.3(1)
Cisco Unified IP Phone 8961, 9951, and 9971	9.3(1)
Cisco Unified Wireless IP Phone 792x Series	1.4(2)
Cisco Unified SIP Phone 3905	9.2(2)

The next sections describe the features for Firmware Release 9.3(1).

- Cisco Unified IP Phones, page 155

Cisco Unified IP Phones

The following table contains the firmware versions for the Cisco Unified IP Phones for Cisco Unified Communications Manager Release 9.0.

Phone family	Release number
Cisco Unified IP Phone 6900 Series	9.3(1)
Cisco Unified IP Phone 7900 Series	9.3(1)
Cisco Unified IP Phone 8941 and 8945	9.3(1)

Phone family	Release number
Cisco Unified IP Phone 8961, 9951, and 9971	9.3(1)
Cisco Unified Wireless IP Phone 792x Series	1.4(2)
Cisco Unified SIP Phone 3905	9.2(2)

The next sections describe the features for Firmware Release 9.3(1).

Cisco Unified IP Phone 6900 Series features

The following table shows the new features that the Cisco Unified IP Phone 6900 Series support with Firmware Release 9.3(1).

Feature	Supported on Cisco Unified IP Phones 6901 and 6911	Supported on Cisco Unified IP Phones 6921, 6941, 6945, and 6961
Device Invoked Recording		X
Extension Mobility Cross Cluster Enhancement		X
Headset Sidetone Control		X
Line Status for Call Lists		X
PLK Support for Queue Status		X
Ring Cadence Localization	X	X
RTCP Behavior On Hold	X	X
View Call Logs From Shared Line		X

The following sections describe the features introduced in Firmware Release 9.3(1) for the Cisco Unified IP Phone 6900 Series.

Device Invoked Recording

The Device Invoked Recording feature enables users to control the recording of phone calls using the Record button on the phone.

Users see a status indicator on the phone display, showing when a conversation is being recorded.

The Device Invoked Recording feature is supported on the following phones (SCCP and SIP):

- Cisco Unified IP Phone 6921

- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to find more information

- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Extension Mobility Cross Cluster Enhancement

The Extension Mobility Cross Cluster (EMCC) Enhancement feature preserves the network and security configurations on the phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC).

The feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to find more information

Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)

Headset Sidetone Control

Headset Sidetone Control lets the user adjust the headset tone levels and can be accessed in the Preferences menu. The users can adjust headset levels to one of the four following settings:

- High
- Normal
- Low
- Off

This feature only applies to wired headsets and does not apply to Bluetooth or wireless headsets.

There is no configuration requirement.

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

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941

- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to find more information

Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)

Line Status for Call Lists

The Line Status for Call Lists feature enables the user to see the availability status of monitored line numbers in the Call History list. The administrator enables or disables this feature using the Line Status for Call Lists parameter in the Enterprise Parameters Configuration window.

When the Line Status for Call Lists parameter is Enabled, the phone line numbers in the Call History register Line Status notifications and an icon appears next to each Call History item in the Call History list. The icon notifies the user that the lines are in one of the following states:

- Idle
- Busy
- DND

When the Line Status for Call Lists parameter is Disabled, the phone line numbers in the Call History list do not register the Line Status notifications.

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

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to find more information

- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

PLK Support for Queue Statistics

The PLK Support for Queue Statistics enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.

The programmable line button Queue Status can be configured by the administrator. When the user presses Queue Status, the phone displays the Queue Status screen. The Queue Status screen includes hunt pilot directory number, number of callers in queue, and the longest call waiting time in queue.

The statistics information is not updated automatically. The user must press the Update button to view updated statistics. To exit from the queue display screen, the user presses the Exit button.

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

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to find more information

- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager (SCCP and SIP)*
- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*

Ring Cadence Localization

The Ring Cadence Localization feature allows IP Phones to use either a North American ring cadence or a Japanese ring cadence. In the Cisco Unified Communications Manager Administration, the administrator sets the Ring Locale field to be either Default or Japan from the Common Profile and phone-specific profile windows.

When Ring Locale is set to Japan, the user does not see the Ringtone entry in the Preferences menu.

The Cisco Unified IP Phone 6901 and 6911 do not have a Preferences menu.

The feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 6901
- Cisco Unified IP Phone 6911
- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to find more information

- *Cisco Unified IP Phone 6901 and 6911 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

RTCP Behavior On Hold

The RTCP Hold For SIP feature ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.

This feature has no administration or user impacts.

The feature is supported on the following SIP phones:

- Cisco Unified IP Phone 6901
- Cisco Unified IP Phone 6911
- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

View Call Logs From Shared Line

The Call History for Shared Line feature offers enhanced viewing of shared line activity in the Cisco Unified IP Phone call history. In addition to logging missed calls for a shared line, this feature will log all answered and placed calls on a shared line.

This feature is supported on the following SIP phones (SCCP and SIP):

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to find more information

- *Cisco Unified IP Phones 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phones 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager Guide 9.0 (SCCP and SIP)*

Cisco Unified IP Phone 7900 Series features

The following table shows the new features that the Cisco Unified IP Phone 7900 Series support with Firmware Release 9.3(1).

Feature	Supported on Cisco Unified IP Phones 7906 and 7911	Supported on Cisco Unified IP Phone 7931	Supported on Cisco Unified IP Phone 7941, 7942, 7961, 7962	Supported on Cisco Unified IP Phone 7945, 7965, 7970, 7971, 7975
Device Invoked Recording	X	X	X	X
Extension Mobility Cross Cluster Enhancement	X	X	X	X
Headset Recording			X (except 7941 and 7961)	X (except 7970 and 7971)
Headset Sidetone Control			X	X
HTTP Firmware Upgrade	X	X	X	X
PLK Support for Queue Status				X
RTCP Behavior On Hold	X	X	X	X
Secure Extension Mobility Cross Cluster	X	X	X	X
SIP Phone No Alert Name	X	X	X	X

The following sections describe the features introduced in Firmware Release 9.3(1) for the Cisco Unified IP Phone 7900 Series.

Device Invoked Recording

The Device Invoked Recording feature enables users to control the recording of phone calls using the Record softkey on the phone.

Users see a status indicator on the phone display, showing when a conversation is being recorded.

The Device Invoked Recording feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 7906G
- 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

Where to find more information

- *Cisco Unified IP Phone 7906G, and 7911G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7906G, and 7911G User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7931G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7931G User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7962G, 7961G-GE, 7961G, 7942G, 7941G-GE, and 7941G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7962G, 7961G-GE, 7961G, 7942G, 7941G-GE, and 7941 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Extension Mobility Cross Cluster Enhancement

The Extension Mobility Cross Cluster (EMCC) Enhancement feature preserves the network and security configurations on the phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC).

The feature is supported on the following SCCP and SIP phones:

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

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

Where to find more information

- *Cisco Unified IP Phone 7906 and 7911 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7931 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7962, 7961, 7942, and 7941 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7975, 7971, 7970, 7965, and 7945 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Headset Recording

The Headset Recording feature adds the audio from the phone handset into the phone headset. If conversations are recorded using the auxilliary port of the headset, the feature ensures that audio from the headset (the agent) and the phone handset (the supervisor) are captured in the recording.

To support this feature, a new field, Headset Recording, is introduced in the Cisco Unified Communications Manager.

For phones associated with Cisco Unified Communications Manager 8.6 and earlier, this feature requires a dev pack.

The feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 7942
- Cisco Unified IP Phone 7945
- Cisco Unified IP Phone 7962
- Cisco Unified IP Phone 7965
- Cisco Unified IP Phone 7975

Where to find more information

- *Cisco Unified IP Phone 7941, 7942, 7961, and 7962 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7945, 7965, 7970, 7971, and 7975 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

HTTP Firmware Upgrade

The HTTP Firmware Upgrade feature enhances the firmware download process by first attempting to download all files using HTTP. If the phone rejects the HTTP connection, the upgrade process uses the existing TFTP download process

There is no user impact to this feature.

The feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 7906
- Cisco Unified IP Phone 7911
- Cisco Unified IP Phone 7931
- Cisco Unified IP Phone 7941
- Cisco Unified IP Phone 7942
- Cisco Unified IP Phone 7945
- Cisco Unified IP Phone 7961
- Cisco Unified IP Phone 7962
- Cisco Unified IP Phone 7965
- Cisco Unified IP Phone 7970
- Cisco Unified IP Phone 7971
- Cisco Unified IP Phone 7975

Where to find more information

- *Cisco Unified IP Phone 7906 and 7911 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7931 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7941, 7942, 7961, and 7962 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7945, 7965, 7970, 7971, and 7975 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

PLK Support for Queue Statistics

The PLK Support for Queue Statistics feature enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.

The programmable line button Queue Status can be configured by the administrator. When the user presses Queue Status, the phone displays the Queue Status screen. The Queue Status screen includes hunt pilot directory number, number of callers in queue, and the longest call waiting time in queue.

The statistics information is not updated automatically. The user must press the Refresh button to view updated statistics. To exit from the queue display screen, the user presses the Exit button.

The feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 7906
- Cisco Unified IP Phone 7911
- Cisco Unified IP Phone 7931
- Cisco Unified IP Phone 7941
- Cisco Unified IP Phone 7942
- Cisco Unified IP Phone 7961
- Cisco Unified IP Phone 7962
- Cisco Unified IP Phone 7965
- Cisco Unified IP Phone 7945
- Cisco Unified IP Phone 7970
- Cisco Unified IP Phone 7971
- Cisco Unified IP Phone 7975

Where to find more information

- *Cisco Unified IP Phone 7945, 7965, 7970, 7971, and 7975 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7945, 7965, 7970, 7971, and 7975 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

RTCP Behavior On Hold

The RTCP Hold For SIP feature ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.

This feature has no administration or user impacts.

The feature is supported on the following SIP phones:

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

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

Where to find more information

- *Cisco Unified IP Phone 7906 and 7911 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7931 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7941, 7942, 7961, and 7962 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 7945, 7965, 7970, 7971, and 7975 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Secure Extension Mobility Cross Cluster

The Secure Extension Mobility Cross Cluster (EMCC) feature enables a user configured in one cluster to log into a Cisco Unified IP Phone in another cluster. The users from a home cluster log into a Cisco Unified IP Phone at a visiting cluster. The visiting cluster can log into home cluster in secure mode.

Configure Cisco Extension Mobility on Cisco Unified IP Phones before you configure EMCC.

The feature is supported on the following phones (SCCP and SIP):

- Cisco Unified IP Phone 7906
- Cisco Unified IP Phone 7911
- Cisco Unified IP Phone 7931
- Cisco Unified IP Phone 7941
- Cisco Unified IP Phone 7942
- Cisco Unified IP Phone 7961
- Cisco Unified IP Phone 7962
- Cisco Unified IP Phone 7965
- Cisco Unified IP Phone 7945

- Cisco Unified IP Phone 7970
- Cisco Unified IP Phone 7971
- Cisco Unified IP Phone 7975

Where to find more information

Cisco Unified Communications Manager Features and Services Guide, chapter "Cisco Extension Mobility Cross Cluster"

Cisco Unified IP Phone 8941 and 8945 features

The following list identifies the new features that the Cisco Unified IP Phone 8941 and 8945 support with Firmware Release 9.3(1).

- Call Log Filter Enhancement
- Extension Mobility Cross Cluster Enhancement
- Headset Sidetone Control
- Line Status for Call Lists
- Pause In Speed Dial
- PLK Support For Queue Statistics
- RTCP Control For Video
- sRTP Secure Video
- SIP Phone No Alert Name
- Secure Extension Mobility Cross Cluster
- Video Disable

The following sections describe the features introduced in Firmware Release 9.3(1) for the Cisco Unified IP Phone 8941 and 8945.

Call Log Filter Enhancement

The Call Log Filter Enhancement feature assists the user make a call by checking the call history as the user dials and presenting a list of entries that match the digits as they are input. The user can select one of the displayed numbers instead of entering the complete telephone number.

To disable call log filtering, the administrator enables the Simplified New Call UI field. By default, call log filtering is enabled.

The feature is supported on the following phones (SCCP and SIP):

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

- *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Device Invoked Recording

The Device Invoked Recording feature enables users to control the recording of phone calls using the Record programmable line key on the phone.

Users see a status indicator on the phone display, showing when a conversation is being recorded.

The Device Invoked Recording feature is supported on the following phones (SCCP and SIP):

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

- *Cisco Unified IP Phone 8941and 8945 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 8941and 8945 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Extension Mobility Cross Cluster Enhancement

The Extension Mobility Cross Cluster (EMCC) Enhancement feature preserves the network and security configurations on the phone. By so doing, security policies are maintained.

The feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)

Headset Sidetone Control

The Headset Sidetone Control feature enables users to adjust the headset sidetone level, from the phone Preference screen. This menu item provides four different headset sidetone levels:

- High
- Normal
- Low

- Off

Note This feature only applies to wired headsets and does not apply to Bluetooth or wireless headsets.

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

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager 9.0.

Line Status for Call Lists

The Line Status for Call Lists feature enables the user to see the availability status of monitored line numbers in the Call History list. The administrator enables or disables this feature using the Line Status for Call Lists parameter in the Enterprise Parameters Configuration window.

When the Line Status for Call Lists parameter is Enabled, the phone line numbers in the Call History register Line Status notifications and an icon appears next to each Call History item in the Call History list. The icon notifies the user that the lines are in one of the following states:

- Unknown
- Idle
- Busy
- DND

When the Line Status for Call Lists parameter is Disabled, the phone line numbers in the Call History list do not register the Line Status notifications.

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

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

- *Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Pause In Speed Dial

The Pause In Speed Dial feature allows users to set up the speed dial feature to reach destinations that require a Forced Authorization Code (FAC), Client Matter Code (CMC), dialing pauses, and additional digits (such

as a user extension, a meeting access code, or a voicemail password) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination with dialing pauses inserted.

To include dialing pauses in the speed dial, the user must specify a comma (,) in the speed dial string. Each comma indicates a pause of 2 seconds. The comma also acts as a delimiter between destination digits, the FAC, CMC, and additional DTMF digits. The comma as delimiter is useful in the following cases:

- Differentiates overlapping dial patterns (for example 9.xxx from 9.xxxxx)
- Differentiates overlapping FAC or CMC (for example, 8787 from 87879)
- Identifies the destination number when using variable-length dial patterns (for example 9.!)

Note Including FAC and CMC in the speed dial string has the following requirements:

- FAC must always precede CMC in the speed dial string.
- A speed dial label is required for speed dials containing FAC and DTMF digits.
- Only one comma is allowed between FAC and CMC digits in the string.

For any additional DTMF digits specified after the FAC and CMC, the phone dials these additional digits (with pauses) after the call is connected.

This feature is supported on the following SIP phones:

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

- *Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manage 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

PLK Support for Queue Statistics

The PLK Support for Queue Statistics feature enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.

The programmable line button Queue Status can be configured by the administrator. When the user presses Queue Status, the phone displays the Queue Status screen. The Queue Status screen includes hunt pilot directory number, number of callers in queue, and the longest call waiting time in queue.

The statistics information is not updated automatically. The user must press the Update button to view updated statistics. To exit from the queue display screen, the user presses the Exit button.

The feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 8941

- Cisco Unified IP Phone 8945

Where to find more information

- *Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager (SCCP and SIP)*
- *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*

RTCP Control for Video

The RTCP Control for Video feature gives the administrator the flexibility to enable the phones to transmit and receive Real-Time Control Protocol (RTCP) packets for both audio and video streams in a video call. Using RTCP, instead of Real Time Transport Protocol (RTP), provides feedback and statistics that assist in phone system support. The protocol choice does not impact the users.

The administrator enables or disables the RTCP for video field from one of the following Cisco Unified Communications Manager windows:

- **Device** > **Phone**
- **Device** > **Device Settings** > **Common Phone Profile**

The feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager 9.0(SCCP and SIP)

sRTP Secure Video

The sRTP Secure Video feature adds more media (audio and video) encryption capabilities and gives the administrator the flexibility to choose RTCP authentication tag length between 32 bit (default) and 80 bit from Cisco Unified CM Administration.

The administrator enables (default) or disables the 80-bit SRTCP field from one of the following Cisco Unified Communications Manager windows:

- **Device** > **Phone**
- **System** > **Enterprise Phone Configuration**
- **Device** > **Device Settings** > **Common Phone Profile**

The feature is supported on the following SIP phones:

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

- *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*
- *Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager (SCCP and SIP)*

SIP Phone No Alert Name

The SIP Phone No Alert Name feature makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The transferred call appears as an Alert Call followed by the caller's telephone number.

This enhancement does not require any specific configuration.

The feature is supported on following phones (SIP only):

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)

Secure Extension Mobility Cross Cluster

The Secure Extension Mobility Cross Cluster (EMCC) feature enables a user configured in one cluster to log into a Cisco Unified IP Phone in another cluster. The users from a home cluster log into a Cisco Unified IP Phone at a visiting cluster. The visiting cluster fails to log into home cluster in secure mode.

Configure Cisco EMCC on the Cisco Unified IP Phones before you configure secure EMCC.

The following table describes the security level of EMCC when both the home and visiting clusters are release 9.0 clusters.

9.0 visiting cluster	9.0 Visiting phone	9.0 home cluster Mixed Mode	9.0 home cluster Nonsecure Mode
Mixed Mode	Secure	Secure EMCC	Log on fails
	Nonsecure	Nonsecure EMCC	Nonsecure EMCC
Nonsecure Mode	Nonsecure	Nonsecure EMCC	Nonsecure EMCC

The following table describes the security level of EMCC when the home cluster is at release 9.0 and the visiting cluster is at release 8.x.

8.x visiting cluster	8.x Visiting phone	9.0 home cluster Mixed Mode	9.0 home cluster Nonsecure Mode
Mixed Mode	Secure	Not supported	Not supported
	Nonsecure	Nonsecure EMCC	Nonsecure EMCC
Nonsecure Mode	Nonsecure	Nonsecure EMCC	Nonsecure EMCC

The following table describes the security level of EMCC when the home cluster is at release 8.x and the visiting cluster is at release 9.0.

9.0 visiting cluster	9.0 Visiting phone	8.x home cluster Mixed Mode	8.7 home cluster Nonsecure Mode
Mixed Mode	Secure	Log on fails	Log on fails
	Nonsecure	Nonsecure EMCC	Nonsecure EMCC
Nonsecure Mode	Nonsecure	Nonsecure EMCC	Nonsecure EMCC

The feature is supported on the following phones (SCCP and SIP):

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

Where to find more information

Cisco Unified Communications Manager Features and Services Guide, chapter "Cisco Extension Mobility Cross Cluster"

Video Disable

The Video Disable feature allows the user to control the sending of video on a call. When the administrator has enabled Video Capability in the Cisco Unified Communications Manager Administration, the user can control the video.

The user sees the Video entry in the Preferences menu, and can enable and disable the ability of the phone to send video.

The feature is supported on the following phones (SCCP and SIP):

- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945

This feature is also supported on third-party telephones.

Where to find more information

- *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*
- *Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Cisco Unified IP Phone 8961, 9951, and 9971 features

The following list identifies the new features that the Cisco Unified IP Phone 8961, 9951, and 9971 support with Firmware Release 9.3(1).

- Default Wallpaper Control
- Device Invoked Recording
- Display SRST Message
- Extension Mobility Cross Cluster Enhancement
- Handset Audio Tuning
- Handset Bass Adjustment
- Line Status for Call Lists
- Pause In Speed Dial
- PLK Support For Queue Statistics
- RTCP Control For Video
- RTCP Hold On SIP
- Secure Extension Mobility Cross Cluster
- Simplified New Call Bubble
- SIP Phone No Alert Name
- Speed Dial Without Restart
- sRTP Secure Video
- Unique Call ID Display
- URI Dialing

The following sections describe the features introduced in Firmware Release 9.3(1) for the Cisco Unified IP Phone 8961, 9951, and 9971.

Assured Services SIP

The Assured Services for SIP Lines (AS-SIP) feature provides the ability for users to place priority calls and, if necessary, preempt lower-priority phone calls.

These AS-SIP enhancements are supported on the following SIP phones:

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

This feature is also supported on third-party telephones.

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*

Device Invoked Recording

The Device Invoked Recording feature enables users to control the recording of phone calls using the Record button on the phone.

Users see a status indicator on the phone display, showing when a conversation is being recorded.

The Device Invoked Recording feature is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)*

Display Survivable Remote Site Telephony Message

The Display Survivable Remote Site Telephony (SRST) Message feature displays a message to the users on the phone screen when communication with the Cisco Unified Communications Manager fails. This message alerts users that some of the features of their phones are no longer available.

This feature is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*

Edit Speed Dial Without Restart

The Speed Dial Without a Restart feature makes it easier maintain an updated collection of Speed Dial numbers by:

- Administrators can add, modify, or delete a Speed Dial number from the Cisco Unified Communications Manager Administration page.
- Users can add, modify, or delete a Speed Dial number from the Cisco Unified Communications Manager User Options web pages.

The phone is not required to restart in order to accept these changes.

This feature does not require any specific configuration.

This enhancement is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*

Extension Mobility Cross Cluster Enhancement

The Extension Mobility Cross Cluster (EMCC) Enhancement feature preserves the Product Specific Configuration settings for the phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC).

The feature is supported on the following SIP phones:

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

Where to find more information

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)

Handset Audio Tuning

Handset Bass Adjustment

The Handset Bass Adjustment feature removes some of the low frequencies on a narrowband handset call, which can improve muffled voices or insufficient volume on handsets. The default setting is for reduced bass.

The feature is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*

Pause In Speed Dial

The Pause in Speed Dial feature enables users to set up the speed dial feature to reach destinations that require a Forced Authorization Code (FAC), Client Matter Code (CMC), dialing pauses, and additional digits (such as a user extension, a meeting access code, or a voicemail password) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination with dialing pauses inserted.

To include dialing pauses in the speed dial, the user must specify a comma (,) in the speed dial string. Each comma indicates a pause of 2 seconds. The comma also acts as a delimiter between destination digits, the FAC, CMC, and additional DTMF digits. The comma as delimiter is useful in the following cases:

- Differentiates overlapping dial patterns (for example 9.xxx from 9.xxxxx)
- Differentiates overlapping FAC or CMC (for example, 8787 from 87879)
- Identifies the destination number when using variable-length dial patterns (for example 9.!)

Be aware of the following requirements when you include FAC and CMC in the speed dial string:

- FAC must always precede CMC in the speed dial string.
- A speed dial label is required for speed dials containing FAC and DTMF digits.
- Only one comma is allowed between FAC and CMC digits in the string.

For any additional DTMF digits specified after the FAC and CMC, the phone dials these additional digits (with pauses) after the call is connected.

This feature is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*

PLK Support for Queue Statistics

The PLK Support for Queue Statistics feature enables the users to query the call queue statistics for hunt pilots and the statistics display on the phone screen.

The programmable line key Queue Status can be configured by the administrator. When the user presses Queue Status, the phone displays the Queue Status screen. The Queue Status screen includes hunt pilot directory number, number of callers in queue, and the longest call waiting time in queue.

The statistics information does not update automatically. The user must press the Update softkey to view updated statistics. To exit from the queue display screen, the user presses the Exit softkey.

The feature is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*

RTCP Hold On SIP

The RTCP Hold For SIP feature ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.

This feature has no administration or user impacts.

The feature is supported on the following SIP phones:

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

RTCP Control for Video

The RTCP Control for Video feature gives the administrator the flexibility to enable the phones to transmit and receive Real Time Control Protocol (RTCP) packets for audio and video streams in a video call. Using RTCP, instead of Real Time Transport Protocol (RTP), provides feedback and statistics that assist in phone system support. The choice of protocol does not impact the users. By default, the feature is disabled.

The administrator enables or disables the RTCP for video field from one of the following Cisco Unified Communications Manager windows:

- **Device** > **Phone**
- **Device** > **Device Settings** > **Common Phone Profile**

The feature is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951,and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*

Secure Extension Mobility Cross Cluster

Secure Extension Mobility Cross Cluster (EMCC) enables a user in one cluster (using an encrypted/authenticated Cisco Unified IP Phone with TFTP Encrypted Config/Digest Authentication enabled) to log in to another cluster when two cluster are both in mixed mode.

Configure Cisco Extension Mobility on Cisco Unified IP Phones before you configure EMCC.

The feature is supported on the following SIP phones:

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

Where to find more information

Cisco Unified Communications Manager Features and Services Guide, chapter "Cisco Extension Mobility Cross Cluster"

Simplified New Call Bubble

The Simplified New Call Bubble feature provides a simplified window for the user to place an off-hook call. The administrator enables or disables the feature in the Phone Configuration window using the Simplified New Call UI field. By default, the feature is disabled.

When the user start dialing a call with the Simplified New Call Window, the phone does not display possible phone number matches from the call history.

The feature is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*

SIP Phone No Alert Name in Placed Calls History

The SIP Phone No Alert Name in Placed Calls History feature displays the alert name in the Placed Calls history when the phone is in a translation pattern or call redirection state. Currently these calls appear on the calling party's call history as Unknown. With this enhancement these calls appear as the callee's Alert Name.

This enhancement does not require any specific configuration.

The feature is supported on following phones (SIP):

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

Where to find more information

Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)

sRTP Secure Video

The sRTP Secure Video feature adds more media (audio and video) encryption capabilities and gives the administrator the flexibility to choose RTCP authentication tag length between 32 bit (default) and 80 bit from Cisco Unified CM Administration.

The administrator enables or disables (default) the 80-bit SRTCP field from one of the following Cisco Unified Communications Manager windows:

- **Device** > **Phone**
- **System** > **Enterprise Phone Configuration**
- **Device** > **Device Settings** > **Common Phone Profile**

The feature is supported on the following SIP phones:

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

This feature has no user impact.

Where to find more information

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)

Unique Call ID Display

The Unique Call ID Display feature ensures that all calls with same group call ID display the same call ID on all the phones with the same shared line DN. Displaying the same call ID on all phones ensures that all users with the same shared line DN can identify the correct active call.

There is no administrator impact to this feature.

The feature is supported on the following SIP phones:

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

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*
- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*

Uniform Resource Identifier Dialing

The Uniform Resource Identifier (URI) Dialing feature enables the user to place calls using alphanumeric URI address as a directory number, for example, bob@cisco.com. The user must enter the URI address to select the contact.

The phone screen displays the call information for the URI call. The call history record the URI call information in the Call History and the Details page.

The user cannot place calls by URI address using the soft keypad.

URI Dialing has the following feature requirements:

Onhook call initiation

The user must press the ABC softkey to switch the input method to URI Dialing mode using the keypad.

Off-hook call initiation

The user can place calls using URI Dialing if the URI address is stored in the speed dial list or call history.

Redial

Press the Redial button to call the most recently dialed URI address.

Speed Dial

The user can configure a URI address as a speed dial entry to place a call.

Session bubble

When the user dials or receives a call through URI Dialing, the call bubble displays the complete URI address.

Incoming call notification

The incoming call alert notification supports the URI address display.

Missed, Placed, and Received call history

The URI Dialing logs are saved in the call history.

Dial URI from call history

The user can select the URI address from the call list to place a call. The user can navigate to the URI call history or enter the URI Dial mode to place a call.

Default domain

The user can enter the complete domain name and override the default domain.

Call History filter

While the user enters the URI address to place a call through URI Dialing, the call history appears based on the characters entered.

Call Forward All

The user can configure the Call Forward All destination using the speed dial or call history entries.

Transfer

The user can initiate a Transfer call using URI dialing if the URI address is stored in the Speed Dial list or Call History.

Ad Hoc Conference

The user can initiate a conference call and add multiple parties using URI Dialing if the URI address is stored in the speed dial list or call history.

Privacy

The user can hide the display of the URI address information. For more information on Privacy, see *Cisco Unified Communications Manager Features and Services Guide 9.0* and *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*.

Busy Lamp Field Speed Dial

The user can monitor the state (in-use or idle) of a call using URI Dialing associated with speed dial or call history.

Call back

The user can initiate a directory number call when the URI Dialing target becomes available.

Features compatibility

The URI address speed dial or redial is disabled under Meet Me conference and Group Call Pickup features.

Cisco Unified Communications Manager Express and Survivable Remote Site Telephony

When the phones are connected to the Cisco Unified Communications Manager Express and Survivable Remote Site Telephony (CME/SRST), the URI Dialing functionalities are disabled. The ABC softkey does not appear on the phone screen.

This feature is supported on the following SIP phones:

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

Note Wait for the ABC softkey to appear before you proceed with URI dialing.

Where to find more information

- *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 9.0 (SIP)*

- *Cisco Unified IP Phone 8961, 9851, and 9971 User Guide for Cisco Unified Communications Manager 9.0 (SIP)*

CHAPTER 5

Other changes

This chapter contains information about other changes introduced to the content for release 9.0 that are not directly related to any new feature. Enter each topic in a separate section. See below.

Cisco Unified Communications Manager License Count Utility

Cisco Unified Communications Manager License Count Utility is a Windows based application that aids administrators to migrate from the Device License Units (DLU) license type to the User Connect License (UCL) license type.

Before you upgrade to a Cisco Unified Communications Manager Release 9.0, download and run the latest version of the Cisco Unified Communications Manager License Count Utility, a nonintrusive tool that enumerates the available DLUs in the Unified CM cluster and, without changing the state of the system, suggests the corresponding UCLs required.

For more information, see the *Using Cisco Unified Communications Manager License Count Utility* .

Video telephony

Cisco Unified Communications Manager Release 9.0 does not support video IPv6 calls. Video always uses IPv4. Video is disabled for any dual-stack or IPv6 audio device that is associated with Cisco Unified Video Advantage.

Unified CM Release 9.0 supports IPv4 only for video streams. Calls between video endpoints and an application must use IPv4 only for both voice and video media streams. Prior to Unified CM Release 9.0, there was the following exception: Cisco Unified Video Advantage, which uses IPv4 exclusively, could be associated with a dual-stack Skinny Client Control Protocol (SCCP) IP phone, forming a composite endpoint which could, in certain circumstances, use IPv6 for voice and, at the same time, IPv4 for video media streams. In Unified CM Release 9.0 and later releases, this exception will no longer be supported, and video will be disabled whenever a dual-stack IP phone configured in dual-stack or IPv6 only mode is associated with Cisco Unified Video Advantage. IP phones that are associated with Cisco Unified Video Advantage must be reconfigured to use IPv4 only for voice, if they are to continue to support video.