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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: 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. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1

About this Release 1

Revision History 1

About Release Notes 1

Cisco Unified Communications Manager, Release 11.0(1a) 2

Documentation for Release 11.0(1) 2

Upgrades 3

Supported Web Browsers 3

CHAPTER 2

Upgrades 5

Software Versions 5

Software Upgrades 5

Preupgrade COP Files 6

Upgrade Restriction from SU1 to SU2 7

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades 7

Cisco Jabber Users Should be Logged Out During Upgrade 8

CHAPTER 3

New and Changed Features 9

Information Assurance Features 9

Enterprise Groups Overview 10

Enable Enterprise Groups 11

View User Groups 12

Managed File Transfer Service Parameters 12

Remove Unused Firmware from the System 13

F5 BIP-IP IDP Support 13

Apply Workaround When Using F5 BIG-IP for SAML SSO 14

Generic Directory Server Support 14
Interoperability 70
   Interoperability with Cisco TelePresence Management Suite 70
   Intercluster Peering Not Supported with Cisco Unified Presence 8.6 70
   SNMP v3 Restriction with FIPS Mode 71
   Tomcat Certificate Regeneration with SAML SSO Deployment 71
Miscellaneous 71
   Bandwidth Allocations for 88xx SIP Phones 71
   Change Perfmon Counter File Size Parameters in RTMT 71
   Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets 71
   IM and Presence Service Ad Hoc Group Chat Rooms Privacy Policy 72
   MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify 73
   Perfect Forward Secrecy is not Supported in IPsec Configuration 73
   Route Filter and Associated Route Patterns 73
   TFTP File Size Limit 73
   IM and Presence Service Persistent Chat Failover Behavior 73
   IM and Presence Service TSnames File Contains Incorrect Details Following Hostname or IP Address Change 73
   Persistent Chat Rooms Using Oracle External Database on IM and Presence Service 74
   IM and Presence Server Pings to Jabber Are Not Configurable 74

CHAPTER 5

New and Retired Documents 75
   New and Retired Documents 75
      Retired Documents 75
   New Documents 76
      System Configuration Guide for Cisco Unified Communications Manager 76
      Feature Configuration Guide for Cisco Unified Communications Manager 77
      Administration Guide for Cisco Unified Communications Manager 77

CHAPTER 6

Documentation Updates for Defects 79
   Administration Guide 79
      Tomcat Certificate and TFTP Service 79
      Insufficient Information About Automatic Fallback 80
      Certificate Monitor Frequency Interval 80
   New System Roles 81
Bulk Certificate Management 81
Bulk Administration Guide 82
   EMCC Device Calculation in the Bulk Administration Tool 82
   Incorrect Text Editor for Creating Text-Based CSV File 82
CDR Admin Guide 82
   Call Termination Cause Codes 82
CDR Analysis and Reporting Administration Guide 86
Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service 86
   Change IP Address or Hostname Using Unified Operating System GUI 86
   Domain Name Change for Cisco Unified Communications Manager 87
      Update Domain Name for Cisco Unified Communications Manager 87
Command Line Interface Reference Guide 87
   utils dbreplication clusterreset 87
   utils ntp server delete 88
Feature Configuration Guide 88
   Add Directory Number to a Device 88
   Cisco IPMA Restriction 88
   Call Back Phone Support for 7800 and 8800 Series 88
   Call Pickup Restriction 89
   Call Transfer to Hunt Pilot Restriction 89
   Cisco Unified Communications Manager Sends INVITE Message to VCS 89
   Client Matter Codes, Forced Authorization Codes, and Failover Calls 89
   Conference Now Restriction 89
   CFUR is not supported by mobile devices 90
   Error in EMCC Secure Service URL Configuration 90
   Client Matter Codes and Force Authorization Codes Not Supported on Cisco Jabber 90
   Incorrect Configuration Example for ASA Router 90
   Incorrect Multicast Music On Hold Restriction 93
   Incorrect Report for Device Mobility 93
   Incorrect URL information for WebDialer 93
   Prerequisite for Private Line Automatic Ringdown Configuration Task Flow for SIP Phones 93
Installing Cisco Unified Communications Manager 94
   Install a New Node in an Existing Cluster 94
SNMP Limits 104
Error in SYSLOG-MIB Parameters 105
Default Alarms in CiscoSyslog File 105
System Configuration Guide 107
Bandwidth Calculations 107
Broadcast Algorithm Restrictions with Call Queuing 107
Common Service Ports 107
Conference Bridges Overview 107
Correction in Software Conference Bridge Maximum Audio Streams 108
FGT not getting updated for end users 108
Insufficient Information About Adding a New ILS Hub 108
Insufficient Information About Third-Party Restrictions 109
Intercluster Lookup Service Name Correction 109
Locations Media Resource Audio Bit Rate Policy Service Parameter Limitation 110
Logical Partition Policy configuration overlap 110
Phone Support for Multilevel Precedence and Preemption 110
Incorrect SSH Password Character Limitation 110
Minimum Call Duration for Quality Report Tool to Collect Streaming Statistics 111
Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager 111
SIP Trunks 111
Time of Day routing not Implemented for Message Waiting Indicator 112
System Error Messages 112
Missing Device Type ENUM Values 112
Missing Reason Codes for LastOutOfServiceInformation Alarms 113
Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager 115
Retrieve Chat Rooms on a Replaced Node 115

CHAPTER 7 Caveats 117
Bug Search Tool 117
Resolved Caveats 118
Open Caveats 118
Caveats 118
Open Caveats for Cisco Unified Communications Manager, Release 11.0(1) 118
Open Caveats for IM and Presence Service, Release 11.0(1) 119
About this Release

- Revision History, on page 1
- About Release Notes, on page 1
- Cisco Unified Communications Manager, Release 11.0(1)a, on page 2
- Documentation for Release 11.0(1), on page 2
- Upgrades, on page 3
- Supported Web Browsers, on page 3

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 06, 2017</td>
<td>Updated information related to documentation defect CSCvg10775.</td>
</tr>
<tr>
<td>October 23, 2017</td>
<td>Added important note on bandwidth allocations for 88xx phones.</td>
</tr>
<tr>
<td>November 2, 2017</td>
<td>Added important note on route filters and associated route patterns.</td>
</tr>
<tr>
<td>December 13, 2017</td>
<td>Added topics on missing ENUM values for CSCvd71818 and CSCvg70867.</td>
</tr>
</tbody>
</table>

About Release Notes

These release notes describe new features, requirements, restrictions, and caveats for Cisco Unified Communications Manager IM and Presence Service. These release notes are updated for every maintenance release but not for patches or hot fixes.

Unified Communications Manager, the call-processing component of the Cisco Unified Communications System, extends enterprise telephony features and capabilities to IP phones, media processing devices, VoIP gateways, mobile devices, and multimedia applications.

The IM and Presence Service collects information about user availability, such as whether users are using communications devices (for example, a phone) at a particular time. IM and Presence Service can also collect information about individual user communication capabilities, such as whether web collaboration or video conferencing is enabled. Applications such as Cisco Jabber and Unified Communications Manager use this
information to improve productivity among employees, that is, to help employees connect with colleagues more efficiently and determine the most effective way to engage in collaborative communication.

Note

In the past, export licenses, government regulations, and import restrictions have limited the ability of Cisco to supply Unified Communications Manager and IM and Presence Service worldwide. Cisco has obtained an unrestricted U.S. export classification to address this issue; IM and Presence Service supports an export unrestricted (XU) version only. The unrestricted version differs from previous releases of IM and Presence Service in that it does not contain strong encryption capabilities.

Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

Cisco Unified Communications Manager, Release 11.0(1)a

Release 11.0(1)a of Cisco Unified Communications Manager provides critical updates to the following high-severity defects that are present with the initial release of Cisco Unified Communications Manager 11.0(1):

• CSCuu84269—Ccm rejects calls via DNS query when FQDN in contact
• CSCuu97800—Core file generated - all phones unregistered

If you are still running Release 11.0(1) of Cisco Unified Communications Manager, and you are impacted by the above defects, there are two possible remedies. To fix your system, perform either of the following tasks:

• Perform a standard upgrade to Release 11.0(1)a—Refer to the Upgrade Guide for Cisco Unified Communications Manager for instructions on how to perform a standard upgrade.

• Download and install the COP file ciscocm.FQDNwithDNS-v1.0.k3.cop from cisco.com. If you install the COP file, you will still be running release 11.0(1), but it will be equivalent to release 11.0(1)a.

Note

These fixes apply to Cisco Unified Communications Manager only. You do not need to upgrade your IM and Presence Service past release 11.0(1) to receive these fixes.

Documentation for Release 11.0(1)

For complete information about this release, refer first to these Release Notes for information about new and changed features in release 11.0(1) and then refer to the Documentation Guide for Cisco Unified Communications Manager and IM and Presence Service Release 11.0(1) at the following URL:

Upgrades

For information about upgrading, as well as requirements for hardware and software, see Install and Upgrade Guides at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html.

Supported Web Browsers

Release 11.0(1) of Cisco Unified Communications Manager has been tested with, and supports the following web browsers:

• Internet Explorer 10 and 11
• Firefox 38
• Chrome 43
• Safari 8

The above web browsers can be used on the following Cisco Unified Communications Manager user interfaces:

• Cisco Unified CM Administration
• Cisco Unified Serviceability
• Cisco Unified Reporting
• CDR Analysis and Reporting
• Disaster Recovery System
• Cisco Unified Communications Self Care Portal
• Cisco Unified Communications Manager Assistant

Please refer to your web browser documentation to determine which platform is supported for your browser.
CHAPTER 2

Upgrades

- Software Versions, on page 5
- Software Upgrades, on page 5
- Preupgrade COP Files, on page 6
- Upgrade Restriction from SU1 to SU2, on page 7
- OS Admin Account Required for CLI-Initiated IM and Presence Upgrades, on page 7
- Cisco Jabber Users Should be Logged Out During Upgrade, on page 8

Software Versions

For Cisco Unified Communications Manager, these release notes are based on the following software version: 11.0.1.10000-10.

For IM and Presence Service, these release notes are based on the following software version: 11.0.1.10000-6.

Software Upgrades

For information about supported upgrades, see the Cisco Unified Communications Manager Compatibility Matrix at the following URL:


Note

All nodes within a single cluster must be in the same mode. For example, Cisco Unified Communications Manager and IM and Presence Service nodes in the same cluster must either all be in unrestricted mode or all be in restricted mode.
Preupgrade COP Files

Installing COP Files from Previous Releases

Release 11.0(1) accepts Cisco Options Package (COP) files that are signed with RSA version 3 keys. If you attempt to install earlier COP files that do not use RSA version 3 keys, the installation will fail. If you need to install COP files from previous releases, such as COP files for older firmware, you can manually upload .ZIP copies of the COP files.

Installing RSA Version 3 Keys on Cisco Unified Communications Manager Nodes

If you are upgrading to Cisco Unified Communications Manager Release 11.0(1) or later, from a release earlier than Cisco Unified Communications Manager Release 10.0(1), you must download and install ciscocm.version3-keys.cop.sgn on every node in the cluster. This Cisco Options Package (COP) file has the RSA keys that are required to validate the upgrade. Missing RSA-3 keys will result in status errors in the Software Installation/Upgrade window of the Cisco Unified Operating System Administration interface.

If you are upgrading to Cisco Unified Communications Manager Release 8.6 or later from a release earlier than Cisco Unified Communications Manager Release 8.5, you must download and install the latest ciscocm.refresh_upgrade_v1.5.cop.sgn on every node in the cluster.


Note

If the ciscocm.version3-keys.cop.sgn file is not installed, then software validation will fail even if the md5sum value of the ISO is correct.

To find COP files on Cisco.com, navigate to Support > Downloads > Cisco Unified Communications Manager Version <version> > Unified Communications Manager/CallManager/Cisco Unity Connection Utilities.

Note

Cisco Prime Collaboration Deployment does not automatically install the required COP file before upgrade. You must create a task in Cisco Prime Collaboration Deployment to install the COP file before the upgrade. For more information, see the Cisco Prime Collaboration Deployment Administration Guide.

Verify that you have the correct COP file installed with the following commands:

```
admin:show version active
Active Master Version: 8.5.1.10000-26
Active Version Installed Software Options:
ciscocm.version3-keys.cop
ciscocm.refresh_upgrade_v1.5.cop.sgn
admin:
```
Installing RSA Version 3 Keys on Cisco Unified Communications Manager on IM and Presence Service Nodes

You must also install the ciscocm.version3-keys.cop.sgn cop file before you upgrade to IM and Presence Service Release 11.0(1) or later, from any release earlier than 10.0(1). This COP file is necessary for all upgrades from pre-10.0(1) to 11.0(1) and later.

Upgrade from Cisco Unified Presence 8.5(4)

For upgrades from Cisco Unified Presence 8.5(4), you must install two COP files in the following order before you begin the upgrade:

1. Install the refresh upgrade COP file, cisco.com.cup.refresh_upgrade_v<latest_version>.cop.
   You can download this COP file from Cisco.com.
2. Install the RSA-3 key COP file, ciscocm.version3-keys.cop.sgn.

Downgrade to Cisco Unified Presence 8.6(3)

Cisco Unified Presence Releases 8.6(4) and later do not support the Cisco Presence Engine database. If you upgrade from Release 8.6(3) to Release 10.5(1) and you subsequently want to revert to Release 8.6(3), you must install a COP file that will reinstall the Cisco Presence Engine database. The COP filename is ciscocm.cup.pe_db_install.cop and you can download it from Cisco.com.

Note

In a multinode environment, you must install the ciscocm.cup.pe_db_install.cop COP file on every node in the cluster after you switch back to Release 8.6(3).

Upgrade Restriction from SU1 to SU2

This information relates to CSCva26416.

Before you upgrade from 11.0(1)SU1 to 110.(1)SU2, verify the names of the following templates and ensure that the names do not contain hyphens or spaces:

- Universal Device Template
- Universal Line Template
- Feature Group Template

You must remove hyphens or spaces from the template names before you begin the upgrade. Hyphens and spaces in template names are not supported and will cause the upgrade to fail.

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades

If you are using the utils system upgrade CLI command to upgrade IM and Presence Service nodes, you must use the default OS admin account, as opposed to a user with administrator privileges. Otherwise, the upgrade will not have the required privilege level to install essential services, thereby causing the upgrade to fail. You can confirm the account’s privilege level by running the show myself CLI command. The account must have privilege level 4.
Please note that this limitation exists for CLI-initiated upgrades of IM and Presence Service only and does not apply to Unified Communications Manager. Also note that this limitation may be fixed for newer ISO files. Refer to your ISO Readme file for details on your specific ISO file. For up to date information on this limitation, see CSCvb14399 at https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvb14399.

**Cisco Jabber Users Should be Logged Out During Upgrade**

When upgrading the IM and Presence Service, it’s best to ensure that all Cisco Jabber users are logged out during the upgrade. The more Cisco Jabber user activity you have, the greater the likelihood that you will receive an error that requires administrator intervention such as a Presence status sync error.
CHAPTER 3

New and Changed Features

• Information Assurance Features, on page 9
• Enterprise Groups Overview, on page 10
• Managed File Transfer Service Parameters, on page 12
• Remove Unused Firmware from the System, on page 13
• F5 BIP-IP IDP Support, on page 13
• Generic Directory Server Support, on page 14
• Opus Codec Support, on page 14
• Interactive Voice Response, on page 15
• Conference Now Calls, on page 19
• Support for Delegated Trust Model in OCSP Response, on page 26
• Delete a Trust Certificate, on page 26
• ECDSA Support for Common Criteria for Certified Solutions, on page 26
• Emergency Call Handler, on page 35
• Quality of Service Updates, on page 47
• Removal of End-to-End RSVP Support, on page 54
• Location-based service on Cisco Emergency Responder, on page 54
• Cisco Unified Communications Manager cache responses to A/AAAA queries, on page 54
• Addition of Second SAST Role in the CTL File for Recovery, on page 62
• SIP Referred by Header, on page 65
• Session ID Header Support, on page 65
• Cisco Endpoints, on page 65

Information Assurance Features

This section describes the new Information Assurance features that were added as part of Cisco Unified Communications Manager Release 11.0(1).

When end users (with either local or LDAP credentials) and administrators log in to web applications for Cisco Unified Communications Manager or IM and Presence Service, the main application window displays the last successful and unsuccessful login details.

Users who log in using the SAML SSO feature can view only the last successful system login information. The user can refer to the Identity Provider (IdP) application to track the unsuccessful SAML SSO login information.
The following web applications display the login attempt information:

- Cisco Unified Communications Manager:
  - Cisco Unified CM Administration
  - Cisco Unified Reporting
  - Cisco Unified Serviceability
- IM and Presence Service
  - Cisco Unified CM IM and Presence Administration
  - Cisco Unified IM and Presence Reporting
  - Cisco Unified IM and Presence Serviceability

Only administrators can log in and view the last login details for the following web applications in Cisco Unified Communications Manager:

- Disaster Recovery System
- Cisco Unified OS Administration

## Enterprise Groups Overview

Cisco Jabber users can search for enterprise groups in Microsoft Active Directory and add them to their contact lists. If a group that is already added to the contact list is updated, the contact list is automatically updated. Cisco Unified Communications Manager synchronizes its database with Microsoft Active Directory groups at specified intervals. The interval at which Cisco Unified Communications Manager synchronizes the groups is determined by the **LDAP Directory Synchronization Schedule** parameters in the **LDAP Directory Configuration** window.

Currently, the Enterprise Groups feature is supported only on the Microsoft Active Directory server. It is not supported on Active Directory Lightweight Directory Services (AD LDS) and other corporate directories.

If a Cisco Jabber user wants to add a group to the contact list while the Enterprise Groups feature is enabled, the Cisco Jabber client sends a group request to the IM and Presence Service node. The IM and Presence Service node provides the following information for each group member:

- Display Name
- User ID
- Title
- Phone number
- Mail ID

**Note**

Only the group members that are assigned to the IM and Presence Service nodes can be added to the contact list. Other group members are discarded.
If you disable the Enterprise Groups feature, Cisco Jabber users cannot search Microsoft Active Directory groups or see the groups that they already added to their contact lists. If a user is already logged in when you disable the Enterprise Groups feature, the group will be visible until the user logs out. When the user logs in again, the group will not be visible.

**Maximum Allowed Entries**

The maximum number of entries that are allowed in a contact list is the sum of the number of entries in the contact list and the number of entries in groups that are already added to the contact list.

Maximum entries in contact list = (number of entries in contact list) + (number of entries in groups)

When the Enterprise Groups feature is enabled, Cisco Jabber users can add the groups to the contact list if the number of entries in the contact list is less than the maximum allowed entries. If the maximum allowed entries is exceeded while the feature is disabled, the users are not restricted until the feature is enabled. If the user continues to be logged in after the feature is enabled, no error message is displayed. When the user logs out and logs in again, an error message is displayed that asks the users to clear the excess entries.

**Related Topics**

- View User Groups

---

### Enable Enterprise Groups

The enterprise parameter Directory Group Operations on Cisco IM and Presence in the Enterprise Parameter Configuration window allows you to enable or disable the Enterprise Groups feature. Follow these steps to enable the Enterprise Groups feature.

**Before you begin**

The Cisco DirSync feature service must be running.

**Procedure**

1. **Step 1**
   - From Cisco Unified CM Administration, choose System > Enterprise Parameters.
   - The Enterprise Parameters Configuration window appears.

2. **Step 2**
   - In the User Management Parameters section, from the Directory Group Operations on Cisco IM and Presence drop-down list, select Enabled.

3. **Step 3** (Optional)
   - From the Syncing Mode for Enterprise Groups drop-down list, choose one of the following:
     - **None**—If you choose this option, the Cisco Intercluster Sync Agent service does not synchronize the enterprise groups and the group membership records between IM and Presence Service clusters.
     - **Differential Sync**—This is the default option. If you choose this option, after all the enterprise groups and group membership records from remote IM and Presence Service clusters are synchronized, the subsequent syncs synchronize only the records that were updated since the last sync occurred.
     - **Full Sync**—If you choose this option, after all the enterprise groups and group membership records from the remote IM and Presence Service clusters are synchronized, all the records are synchronized during each subsequent sync.
If the Cisco Intercluster Sync Agent service is not running for more than 24 hours, we recommend that you select the **Full Sync** option to ensure that the enterprise groups and group membership records synchronize completely. After all the records are synchronized, that is, when the Cisco Intercluster Sync Agent has been running for about 30 minutes, choose the **Differential Sync** option for the subsequent syncs. Keeping the value of this parameter set to 'Full Sync' for a longer period could result in extensive CPU usage and therefore we recommend that you use the **Full Sync** option during off-business hours.

**Step 4**  
(Optional) Set the **LDAP Directory Synchronization Schedule** parameters in the **LDAP Directory Configuration** window to configure the interval at which Microsoft Active Directory groups are synchronized with Cisco Unified Communications Manager. For more information, see the online help.

**Step 5**  
Click **Save**.

---

**What to do next**

(Optional) **View User Groups, on page 12.**

### View User Groups

You can view the Active Directory user groups that are synchronized with the Cisco Unified Communications Manager database using the following steps.

**Procedure**

1. **Step 1** From Cisco Unified CM Administration, choose **User Management > User Settings > User Group**. The **Find and List User Groups** window appears.
2. **Step 2** Enter search criteria and click **Find**. A list of user groups that match the search criteria is displayed.
3. **Step 3** To view a list of users that belong to a user group, click on the required user group. The **User Group Configuration** window appears.
4. **Step 4** Enter search criteria and click **Find**. A list of users that match the search criteria is displayed.

If you click on a user in the list, the **End User Configuration** window appears.

---

### Managed File Transfer Service Parameters

To help you to manage the external file server disk space, you can define the thresholds at which an RTMT alarm is generated with the following service parameters (for the Cisco XCP File Transfer Manager service):

- **External File Server Available Space Lower Threshold**—If the percentage of available space on the external file server partition is at or below this value, the XcpMFTExtFsFreeSpaceWarn alarm is raised. The default value for this service parameter is 10%.
• **External File Server Available Space Upper Threshold**—If the percentage of available space on the external file server partition reaches or exceeds this value, the XcpMFTExtFsFreeSpaceWarn alarm is cleared. The default value for this service parameter is 15%.

You must restart the Cisco XCP Router service after you change either of these parameters. To configure these parameters, log in to the Cisco Unified CM IM and Presence Administration interface, choose **System > Service Parameters**, and select the Cisco XCP File Transfer Manager service for the node.

---

**Tip**

Do not configure the lower threshold value to be greater than the upper threshold value. Otherwise the Cisco XCP File Transfer Manager service will not start after you restart the Cisco XCP Router service.

---

**Remove Unused Firmware from the System**

The **Device Load Management** window allows you to delete unused firmware (device loads) and associated files from the system to increase disk space. For example, you can delete unused loads before an upgrade to prevent upgrade failures due to insufficient disk space. Some firmware files may have dependent files that are not listed in the **Device Load Management** window. When you delete a firmware, the dependent files are also deleted. However, the dependent files are not deleted if they are associated with additional firmware.

---

**Note**

You must delete unused firmware separately for each server in the cluster.

---

**Before you begin**

**Caution**

Before you delete unused firmware, ensure that you are deleting the right loads. The deleted loads cannot be retrieved. We recommend that you take a backup before deleting the firmware.

---

**Procedure**

1. **Step 1**
   From Cisco Unified OS Administration, choose **Software Upgrades > Device Load Management**.
2. **Step 2**
   Specify the search criteria and click **Find**.
3. **Step 3**
   Select the device load that you want to delete. You can select multiple loads if required.
4. **Step 4**
   Click **Delete Selected Loads**.
5. **Step 5**
   Click **OK**.

---

**F5 BIP-IP IDP Support**

Cisco Unified Communications Manager Release 11.0(1) tests the SSO functionality and SAML 2.0 interface with F5 BIG-IP as the Identity Provider.
Apply Workaround When Using F5 BIG-IP for SAML SSO

While testing the SSO functionality on SAML 2.0 interface with F5 BIG-IP, we discovered that F5 BIG-IP may need an adjustment to comply with the SAML 2.0 standard. This issue is currently being addressed by F5 BIG-IP. In the meantime, you can use this temporary workaround to modify the metadata from F5 BIG-IP IDP. Contact your IDP provider for more details about F5 BIG-IP configuration.

Follow these steps before uploading metadata from F5 BIG-IP to Cisco Unified Communications Manager:

Procedure

- **Step 1**: Using an XML editor, open the exported F5 BIG-IP IDP metadata XML file.
- **Step 2**: From the NameIDFormat tag, delete the following attributes:
  
  ```xml
  <NameIDFormat isDefault="true" index="0"
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP">
  </NameIDFormat>
  ```

- **Step 3**: From the SingleSignOnService tag, delete Index and IsDefault attributes.
- **Step 4**: From the SingleLogOutService tag, delete the IsDefault attribute.
- **Step 5**: In the IDPSSODescriptor tag, change the order of the tags as follows:
  
  1. KeyDescriptor
  2. SingleLogoutService
  3. NameIDFormat
  4. SingleSignOnService
  5. saml:Attribute

- **Step 6**: Save the file.

Generic Directory Server Support

Starting with Release 11.0(1), you can use LDAPv3-compliant directories with Cisco Unified Communications Manager.

Opus Codec Support

This section describes the new Opus codec support that was added as part of Cisco Unified Communications Manager Release 11.0(1).

Opus codec is an interactive speech and audio codec that is, specially designed to handle a wide range of interactive audio applications such as VoIP, video conferencing, in-game chat, and live distributed music performance.

This codec scales from narrowband low bit rate to a very high-quality bit rate ranging from 6 to 510 kb/s.

Opus is supported for SIP devices. The Opus codec service parameter **Opus Codec Enabled** is set to **Enabled for All Devices** by default. The service parameter settings is configured to enable Opus codec for all nonrecording devices or is set to **Disabled** in the **Service Parameter Configuration** window.
### Interactive Voice Response

The following sections describe the new Interactive Voice Response (IVR) feature that was added as part of Cisco Unified Communications Manager Release 11.0(1).

#### Interactive Voice Response Overview

The Interactive Voice Response (IVR) device enables Cisco Unified Communications Manager to play prerecorded feature announcements (.wav files) to devices such as Cisco Unified IP Phones and Gateways. These announcements play on devices that use features which require IVR announcements, like Conference Now.

When you add a node, an IVR device is automatically added to that node. The IVR device remains inactive until the Cisco IP Voice Media Streaming Application service is activated on that node.

An IVR supports 48 simultaneous callers by default. You can change the number of IVR callers using the Cisco IP Voice Media Streaming Application service parameter. However, we recommend that you do not exceed 48 IVR callers on a node. You can configure the number of callers for IVR based on expected simultaneous calls to IVR for joining Conference Now.

⚠️ **Caution**

Do not activate the IVR device on Cisco Unified Communications Manager nodes that have a high call-processing load.

#### Default Announcements and Tones

Cisco Unified Communications Manager automatically provides a set of prerecorded Interactive Voice Response (IVR) announcements when you activate the Cisco IP Media Streaming Application service. You can replace the default prerecorded IVR announcements. An announcement is played for the following conditions:
Table 3: Prerecorded IVR Announcements

<table>
<thead>
<tr>
<th>Announcement</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConferenceNowAccessCodeFailed Announcement</td>
<td>Plays when an attendee enters the wrong access code to join Conference Now after exceeding the maximum number of attempts.</td>
</tr>
<tr>
<td>ConferenceNowAccessCodeInvalid Announcement</td>
<td>Plays when an attendee enters the wrong access code.</td>
</tr>
<tr>
<td>ConferenceNowCFBFailed Announcement</td>
<td>Plays when the conference bridge capacity limit is exceeded while initiating Conference Now.</td>
</tr>
<tr>
<td>ConferenceNowEnterAccessCode Announcement</td>
<td>Plays when an attendee joins Conference Now and the host sets an attendee access code.</td>
</tr>
<tr>
<td>ConferenceNowEnterPIN Announcement</td>
<td>Plays when a host or attendee tries to join a meeting.</td>
</tr>
<tr>
<td>ConferenceNowFailedPIN Announcement</td>
<td>Plays after the host exceeds the maximum number of attempts to enter a correct PIN.</td>
</tr>
<tr>
<td>ConferenceNowGreeting Announcement</td>
<td>Plays a greeting prompt for Conference Now.</td>
</tr>
<tr>
<td>ConferenceNowInvalidPIN Announcement</td>
<td>Plays when the host enters a wrong PIN.</td>
</tr>
<tr>
<td>ConferenceNowNumberFailed Announcement</td>
<td>Plays when a host or attendee enters the wrong meeting number after exceeding the maximum number of attempts.</td>
</tr>
<tr>
<td>ConferenceNowNumberInvalid Announcement</td>
<td>Plays when a host or attendee enters a wrong meeting number.</td>
</tr>
</tbody>
</table>

Interactive Voice Response Restrictions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>IVR</td>
<td>The Interactive Voice Response (IVR) uses Real-Time Protocol (RTP) streams through a common media device driver. This device driver is also used by other software media devices provided by the Cisco IP Voice Media Streaming Application services such as Music On Hold (MOH), Software Media Termination Point (MTP), Software Conference Bridge (CFB), and Annunciator. Configuring more number of calls on a device affects the system performance. This also impacts call processing if the Call Manager service is active on the same server node.</td>
</tr>
<tr>
<td>IVR</td>
<td>The IVR supports only Out-Of-Band (OOB) DTMF digit collection method. If there is a DTMF capability mismatch between the calling device and the IVR, an MTP will be allocated.</td>
</tr>
</tbody>
</table>
The IVR only supports codec G.711 (a-law and mu-law), G.729, and Wide Band 256k. If there is a codec mismatch between the calling device and the IVR, a transcoder will be allocated.

### Interactive Voice Response Configuration Task Flow

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activate the Interactive Voice Response, on page 17</strong></td>
<td></td>
<td>Activate the Cisco IP Voice Media Streaming Application service on the node to activate the IVR for that node. Activate only one Cisco IP Voice Media Streaming Application service for each IVR device in the cluster.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required: View List of Media Resource Groups That Have IVR, on page 18</strong></td>
<td></td>
<td>Add the IVR to media resource groups and lists to manage your media resources using Cisco Unified Communications Manager Administration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(Optional) Change the Default Number of Media Streams</strong></td>
<td></td>
<td>You can change the default number of media streams for an IVR.</td>
</tr>
</tbody>
</table>

#### Activate the Interactive Voice Response

Activate one or more Cisco IP Voice Media Streaming Application service for each node to have Interactive Voice Response (IVR) device registered in the cluster.

⚠️ **Caution**

Do not activate the IVR on Cisco Unified Communications Manager nodes that have a high call-processing load.

#### Procedure

**Step 1**

From the Cisco Unified Serviceability GUI, choose **Tools > Activation.** The **Service Activation** window appears.

**Step 2**

Select the node in the **Server** field and click **Go.**

**Step 3**

Check the **Cisco IP Voice Media Streaming Application** check box, and then click **Save.**
**View List of Media Resource Groups That Have IVR**

**Procedure**

**Step 1**  
From Cisco Unified CM Administration, choose **Media Resources** > **Interactive Voice Response (IVR)**. 
The **Find and List Interactive Voice Response (IVR)** window is displayed.

**Step 2**  
From the **Find and List Interactive Voice Response (IVR) where** window, click **Find**. 
A list of IVRs that are available on Cisco Unified Communications Manager is displayed.

**Step 3**  
Choose the IVR on which you want to see the associated list of media resource groups.

**Step 4**  
Choose **Dependency Records** from the **Related Links** drop-down list and click **Go**. 
If the dependency records are not enabled for the system, the **Dependency Records Summary** window displays a message.

**IVR Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The system automatically displays the preconfigured server (servers are added at installation).</td>
</tr>
<tr>
<td>Name</td>
<td>This field designates the name that is used when the device registers with the Cisco Unified Communications Manager. Enter a name of up to 15 alphanumeric characters (you can use periods, dashes, and underscores).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of up to 128 alphanumeric characters (you can use periods, dashes, and underscores). Default uses the server name, which includes the prefix IVR_.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose Default or choose a device pool from the drop-down list of configured device pools.</td>
</tr>
</tbody>
</table>
| Location     | Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC allows you to regulate audio quality and video availability by limiting the bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. 

From the drop-down list, choose the appropriate location for this IVR.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this IVR consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the **System > Location** menu option.

For details on setting up a location-based CAC across intercluster trunks, see the [System Configuration Guide for Cisco Unified Communications Manager](#).
From the drop-down list, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:

- Off—Choose this value to disable the use of a TRP with this device.
- On—Choose this value to enable the use of a TRP with this device.

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Cisco Unified Communications Manager 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.

If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager searches for an RSVPAgent that can also be used as a TRP.

If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager searches for a transcoder that is also designated as a TRP.

### Change IVR Parameters

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Service Parameters. The Service Parameters Configuration window appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the server and then select the service called Cisco IP Voice Media Streaming App. The Service Parameter Configuration window appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the number of simultaneous media streams in the Call Count field of the Interactive Voice Response (IVR) Parameters section, and then click Save. When you update the IVR, the changes automatically occur when the IVR is idle and no active announcements are playing.</td>
</tr>
</tbody>
</table>

### Conference Now Calls

The following sections describe the new Conference Now feature that was added as part of Cisco Unified Communications Manager Release 11.0(1).
Conference Now Overview

The Conference Now feature allows both external and internal callers to join a conference by dialing a Conference Now IVR Directory Number, which is a centralized conference assistant number. An IVR application guides the caller to join the conference by playing announcements.

A conference is established using a Meeting Number, which is the same as the Self-Service User ID. The meeting number is configured by the administrator in the end user's window. The Self-Service User ID is usually same as the user's primary extension number.

The host (End User) provides the Meeting Number, Time slot, and Attendees Access Code to all the participants. The host requires a PIN to join the conference, but the participants do not require it. If a participant dials into the meeting before the host, the participant hears Music on Hold (MOH).

After the host enters both Meeting Number and PIN correctly, a conference bridge is allocated based on the MRGL (Media Resource Group List) of the host. Participants who join before the start of the meeting are redirected to the same conference bridge.

The host can set the Attendees Access Code for a secure conference call. For more information, see topics related to Set the Access Code for Conference Now in the Cisco Unified Communications Self Care Portal Guide.

Conference Now Prerequisites

To use Conference Now you must make sure that the following media resources are configured, and are available to the devices that will be initiating conferences.

- Conference Bridge—For the best user experience, we recommend using a software-based Cisco IPVMS conference bridge. Using another conference bridge might not provide the conference party entry and exit tone.
- Interactive Voice Response (IVR)

After you configure these resources, you can make them available to devices by configuring a media resource group list that includes these resources and then associating that media resource group list to the device pools that will be used by your devices, or to individual devices. For details on configuring Conference Bridges, Interactive Voice Response, and Media Resource Groups, see the "Configure Media Resources" section of the System Configuration Guide for Cisco Unified Communications Manager.

Conference Now Task Flow

Before you begin

- Review Conference Now Prerequisites, on page 20.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>To host a conference, enable the option in the Feature Group Template.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add a Quick User/Phone, on page 21</td>
<td>(Optional) Use to add a new user.</td>
<td></td>
</tr>
</tbody>
</table>
Enable End User to Host Conference Now

Procedure

Step 1  From Cisco Unified CM Administration, choose User Management > User/Phone Add > Feature Group Template.
        The Find and List Feature Group Templates window appears.
Step 2  Enter the appropriate search criteria and click Find.
        All matching records are displayed.
Step 3  In the list of records, click the link for the record that you want to view.
        The Feature Group Template Configuration window appears.
Step 4  Check the Enable End User to Host Conference Now check box in the Features section to allow the user to host a conference.
Step 5  Click Save.

What to do next

Add a Quick User/Phone, on page 21

Add a Quick User/Phone

Before you begin

Enable End User to Host Conference Now, on page 21

Procedure

Step 1  From Cisco Unified CM Administration, choose User Management > User/Phone Add > Quick User/Phone Add.
        Find and List Users window is displayed.
Step 2  Click Add New.
Step 3  Configure the fields in the Quick User/Phone Add window. For more information about the fields and their configuration options, see the online help.
Step 4  Click Save.

What to do next

(Optional) Configure End User to Host Conference Now, on page 22
Configure End User to Host Conference Now

Procedure

**Step 1** From Cisco Unified CM Administration, choose User Management &gt; End User. The Find and List Users window is displayed.

**Step 2** To select an existing user, specify the appropriate filters in the Find User Where field, click Find to retrieve a list of users, and then select the user from the list. The search result displays all the end users that are configured in Cisco Unified Communications Manager.

**Step 3** Click on the username to display user information. The End User Configuration window is displayed.

**Step 4** Locate the Conference Now Information section.

**Step 5** Check the Enable End User to Host Conference Now check box. If Enable End User to Host Conference Now is enabled under the Feature Group Template, then the newly added user inherits the default settings.

**Step 6** The Meeting Number is generated automatically when the Self-Service User ID field in the End User Configuration window is configured. This number is the default directory number of the user which is modified in the Self-Service User ID field.

**Step 7** (Optional) Enter the Attendees Access Code. The host can set the Attendees Access Code for a secure conference call. Later, the user can modify the access code in the Self Care Portal. For more information about configuration fields, see the Cisco Unified Communications Self Care Portal User Guide.

**Step 8** Click Save.

What to do next

Configure Conference Now, on page 22

Configure Conference Now

**Before you begin**

Configure End User to Host Conference Now, on page 22

**Procedure**

**Step 1** From Cisco Unified CM Administration, choose Call Routing &gt; Conference Now. The Conference Now Configuration window appears.

**Step 2** Configure the fields in the Conference Now Configuration window. For more information about the fields and their configuration options, see the Related Topics section.

**Step 3** Click Save.
### Conference Now Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Now IVR Directory Number</td>
<td>Enter a DID (Direct Inward Dial) number for a Cisco Unified Communications Manager cluster so that external callers can access this number. The combined number and partition must be unique within a cluster.</td>
</tr>
<tr>
<td>Route Partition</td>
<td>To use a partition to restrict access to the Conference Now number or pattern, choose the desired partition from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>If you do not want to restrict access to the Conference Now number or pattern, choose &lt;None&gt; for the partition.</td>
</tr>
<tr>
<td></td>
<td>You can configure the number of partitions that are displayed in this drop-down list by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the <strong>Find</strong> button is displayed next to the drop-down list box. Click the <strong>Find</strong> button to display the <strong>Find and List Partitions</strong> window.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To set the maximum list box items, choose <strong>System &gt; Enterprise Parameters</strong> and update the Max List Box Items field under CCMAadmin Parameters.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Make sure that the combination of Conference Now number or pattern and partition is unique within the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>The description can include up to 50 characters in any language, but it cannot include double quotation marks (&quot;), percentage sign (%), ampersand (&amp;), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Maximum Wait Time For Host Until Participant is Disconnected</td>
<td>Select an integer value to set the maximum wait time, in minutes, in a queue. The default value is 15 minutes. The field range is from 1 to 60 minutes</td>
</tr>
<tr>
<td></td>
<td>This field specifies the maximum wait time for an attendee before a host joins the meeting.</td>
</tr>
<tr>
<td></td>
<td>If the host has not yet joined the meeting after the timer expires, the attendee is disconnected automatically.</td>
</tr>
</tbody>
</table>
MOH Source While Participant is Waiting

Choose a Music On Hold (MOH) source from the drop-down list. The default value is NULL.

If nothing is selected, the default Network Hold MOH/MOH Source configured on the service parameter is used.

The MOH source is configured as unicast or multicast. The media resource group list (MRGL) configuration of the caller takes precedence for multicast or unicast.

When any of the MOH settings are changed, the existing callers who are waiting in the queue are not affected.

All future callers in the queue will listen to MOH as per the updated settings.

### Conference Now Interactions and Restrictions

#### Conference Now Interactions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interactions</th>
</tr>
</thead>
</table>
| Mobility EFA (Enterprise Feature Access) | A mobility user dials an Enterprise Feature Access DID number from a remote destination. After the call is connected, the remote destination phone is used to send DTMF digits to Cisco Unified Communications Manager via the PSTN gateway. 

The user PIN followed by the # key is first authenticated with Cisco Unified Communications Manager. After the user PIN authentication is successful, press 1 and the # key, to indicate a two-stage dialed call, followed by the desired phone number. If the dialed phone number is a Conference Now IVR Directory Number and the user is a meeting host, then the user must enter the PIN again. |

| Mobility MVA (Mobile Voice Access) | A call is directed to Cisco Unified Communications Manager through the enterprise PSTN H.323 or SIP gateway. The IVR prompts the user to enter the User ID, # key, PIN, # key, number 1 (to make a Mobile Voice Access call) and then the desired phone number. If the phone number is a Conference Now IVR Directory Number and the user is a meeting host, then the user must enter the PIN again. 

**Note** Users are not prompted for entering their PIN if they dial directly from their remote destination. However, if they dial from a different phone to Mobile Voice Access Directory Number, then they are prompted to enter PIN before they can make the call. If the users call Conference Now IVR Directory Number, they are prompted to enter the PIN again. |

#### Conference Now Restrictions

The Conference Now feature has the following restrictions:

- The host cannot mute attendees.

- The attendee cannot mute the audio by entering DTMF digits.

- The list of Conference Now participants is not supported.
• Maximum number of participants in a conference is controlled by the existing CallManager service parameter "Maximum MeetMe Conference Unicast". It applies to both internal and external callers.

• Maximum number of simultaneous Conference Now and MeetMe conference instances combined together is 100 per Cisco Unified Communications Manager CallManager node.

• Video on hold is not supported.

• The IPVMS software conference bridge only supports codec G.711 (ALaw & ULaw) and Wide Band 256k. If there is a codec mismatch between the calling device and the software conference bridge, a transcoder will be allocated.

• Ensure that at least one of the following conditions are met to play the conference party entry and exit tone:
  - At least one conference participant is using the Cisco IP Phone.
  - IPVMS is the allocated software conference bridge.

• When the sets up a Conference Bridge, the conference will continue with the remaining attendees irrespective whether the host is present or not. If the host wants to rejoin the conference, an announcement to enter the Attendee Access Code is played if it is configured by host. The host cannot schedule or mute attendees; therefore, the host status is no longer valid.

• No audio announcement will play if the host is the first person to join the conference. However, when the host dials into Conference Now from an internal IP Phone, there is a visual display on the IP Phone showing “To Conference”.

  Note If the host joins the Conference Now from any external phone, then there will be no visual display on the phone.

### Set the Access Code for Conference Now

The new Access Code must be between 3 and 10 digits. It cannot include spaces, letters, or special characters. To reset the Access Code, perform the following steps:

#### Procedure

1. Click the **General Settings** tab.
2. Click **Conference Now**.
3. In the **Attendees Access Code** text box, enter the new Access Code.
4. Click **Save**.
Support for Delegated Trust Model in OCSP Response

Cisco Unified Communications Manager Release 11.0 supports Online Certificate Status Protocol (OCSP), which allows a device to obtain real-time information about the status of a certificate. Examples of certificate status are Good, Revoked, and Unknown.

Cisco Unified Communications Manager uses OCSP for validating third-party certificates that are uploaded into the Cisco Unified Communications Manager trust store. Cisco Unified Communications Manager requires an OCSP Responder URL to connect to the OCSP responder server over HTTP. It sends an HTTP request to the responder to validate a certificate.

Delete a Trust Certificate

For Release 11.0(1) of Cisco Unified Communications Manager, the following note is added in the procedure.

Note

If the certificate that you delete is of the type “tomcat-trust”, “CallManager-trust” or “Phone-SAST-trust”, the certificate is deleted across all servers in the cluster.

ECDSA Support for Common Criteria for Certified Solutions

Unified Communications Manager supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. These certificates are stronger than the RSA-based certificates and are required for products that have Common Criteria (CC) certifications. The US government Commercial Solutions for Classified Systems (CSfC) program requires the CC certification and so, it is included in Unified Communications Manager.

The ECDSA certificates are available along with the existing RSA certificates in the following areas—Certificate Manager, SIP, Certificate Authority Proxy Function (CAPF), Transport Layer Security (TLS) Tracing, Entropy, HTTP, and computer telephony integration (CTI) Manager.

Certificate Manager ECDSA Support

In Unified Communications Manager Release 11.0, the certificate manager supports both generation of self-signed ECDSA certificates and the ECDSA certificate signing request (CSR). Earlier releases of Unified Communications Manager supported RSA certificate only. However, Unified Communications Manager Release 11.0 onwards, CallManager-ECDSA certificate has been added along with the existing RSA certificate.

Both the CallManager and CallManager-ECDSA certificates share the common certificate trust store—CallManager-Trust. Unified Communications Manager uploads these certificates to this trust store.

The certificate manager supports generation of ECDSA certificates having different values of key length.

When you update or install Unified Communications Manager, the self-signed certificate is generated. Unified Communications Manager Release 11.0 always has an ECDSA certificate and uses that certificate in its SIP interface. The secure Computer Telephony Integration (CTI) Manager interface also supports ECDSA.
certificates. As both the CTI Manager and SIP server use the same server certificate, both the interfaces work in synchronization.

**SIP ECDSA Support**

Unified Communications Manager Release 11.0 includes ECDSA support for SIP lines and SIP trunk interfaces. The connection between Unified Communications Manager and an endpoint phone or video device is a SIP line connection whereas the connection between two Unified Communications Managers is a SIP trunk connection. All SIP connections support the ECDSA ciphers and use ECDSA certificates.

Following are the scenarios when SIP makes (Transport Layer Security) TLS connections:

- **When SIP acts as a TLS server**—When the SIP trunk interface of Unified Communications Manager acts as a TLS server for incoming secure SIP connection, the SIP trunk interface determines if the CallManager-ECDSA certificate exists on disk. If the certificate exists on the disk, the SIP trunk interface uses the CallManager-ECDSA certificate if the selected cipher suite is
  
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

  The SIP trunk interface continues to support RSA TLS cipher suites for connections from clients that do not support ECDSA cipher suites. The **TLS Ciphers** drop-down list contains options that permit configuration of the supported cipher suites when Unified Communications Manager acts as a TLS server.

- **When SIP acts as a TLS client**—When the SIP trunk interface acts as a TLS client, the SIP trunk interface sends a list of requested cipher suites to the server based on the **TLS Ciphers** field (which also includes the **ECDSA ciphers** option) in the **Enterprise Parameters** window of Cisco Unified Communications Manager. The **TLS Ciphers**. This configuration determines the TLS client cipher suite list and the supported cipher suites in order of preference.

**Note**

If you establish a TLS connection with an earlier release of the Unified Communications Manager that does not support ECDSA client certificate, the connection uses an RSA cipher suite. The client certificate sent in the TLS connection is not bound to the TLS Cipher you that you choose. Earlier releases of Unified Communications Manager also support that TLS servers receive and handle ECDSA client certificates.

Devices that use an ECDSA cipher to make a connection to Unified Communications Manager must have the CallManager-ECDSA certificate in their Identity Trust List (ITL) file. Then, the devices must incorporate the CallManager-ECDSA certificate into their local certificate store to trust the connection that is secured by the CallManager-ECDSA certificate.

**CAPF ECDSA Support**

Certificate Authority Proxy Function (CAPF) is a Cisco proprietary method for exchanging certificates between Cisco endpoints and Unified Communications Manager. Only Cisco endpoints use CAPF. To accomplish common criteria requirements, CAPF is updated to CAPF version 3 so that a client can be provided with ECDSA Locally Significant Certificate (LSC). A customer creates LSC locally. An LSC is an alternative to manufacturer installed certificate (MIC) that the manufacturer creates.

Use CAPF version 3 to allow Unified Communications Manager server to direct phone, CTI applications, and Jabber clients to generate EC keys to be used in their LSCs. After the EC Keys are generated, Unified
Communications Manager either generates an ECDSA LSC and sends it to the Cisco endpoint or generates an ECDSA CSR.

In case the endpoint does not have CAPF version 3 support, you can configure the required EC key size and RSA key size and choose EC Key Preferred, RSA Backup option in Phone Configuration window from Cisco Unified CM Administration as a backup. This backup option is useful when CAPF server tries to send a request to EC key pair and the phone communicates to the server that it does not support EC key, the server sends the request to generate an RSA key pair instead of the EC key pair.

---

**Note**

Currently, no Cisco endpoint supports CAPF version 3. So, avoid selecting the EC Only option. However, the administrators who want to support ECDSA LSCs later can configure their devices with EC Preferred RSA Backup option. When the endpoints begin to support CAPF version 3 for ECDSA LSCs, the administrators need to reinstall their LSC.

---

**Note**

The Endpoint Advanced Encryption Algorithms Support parameter indicates that phones download the TFTP configuration files using advanced TLS ciphers. By default, EC ciphers have the highest priority. This solution is only supported for an on-premises deployment without MRA.

---

**TLS Tracing**

Cisco Unified Communications Manager Release 11.0 onwards, you can enable or disable TLS tracing for services. Currently, Tomcat is the only supported service. Use the CLI commands to view the reasons of connection failure of TLS connections to Cisco Unified Communications Manager.

**CLI Commands**

Following TLS-based CLI commands are added for TLS tracing:

```plaintext
set tlstrace enable
```

This CLI command enables the TLS tracing for a service.

```
set tlstrace enable service
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Specifies the service that you use to enable TLS tracing.</td>
</tr>
</tbody>
</table>

**Command Modes**

Administrator (admin:)

**Example**

```
admin:set tlstrace enable tomcat
TLS tracing is enabled for: tomcat
```
**Requirements**

Command privilege level: 1  
Allowed during upgrade: No

**set tlstrace disable**

This CLI command disables the TLS tracing for a service.

**set tlstrace disable service**

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Specifies the service that you use to disable TLS tracing.</td>
</tr>
</tbody>
</table>

**Command Modes**

Administrator (admin:)

**Example**

```
admin: set tlstrace disable tomcat  
TLS tracing is disabled for: tomcat
```

**Requirements**

Command privilege level: 1  
Allowed during upgrade: No

---

**Entropy**

To have strong encryption, a robust source of entropy is required. Entropy is a measure of randomness of data and helps in determining the minimum threshold for common criteria requirements. Data conversion techniques, such as cryptography and encryption, rely on a good source of entropy for their effectiveness. If a strong encryption algorithm, such as ECDSA, uses a weak source of entropy, the encryption can be easily broken.

In Unified Communications Manager Release 11.0, the entropy source for Unified Communications Manager is improved. Entropy Monitoring Daemon is a built-in feature that does not require configuration. However, you can turn it off through the Unified Communications Manager CLI.

Use the following CLI commands to control the Entropy Monitoring Daemon service:

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>utils service start Entropy Monitoring Daemon</code></td>
<td>Starts the Entropy Monitoring Daemon service.</td>
</tr>
<tr>
<td><code>utils service stop Entropy Monitoring Daemon</code></td>
<td>Stops the Entropy Monitoring Daemon service.</td>
</tr>
<tr>
<td><code>utils service active Entropy Monitoring Daemon</code></td>
<td>Activates the Entropy Monitoring Daemon service, which further loads the kernel module.</td>
</tr>
</tbody>
</table>
### CLI Command

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>utils service deactive Entropy Monitoring Daemon</code></td>
<td>Deactivates the Entropy Monitoring Daemon service, which further unloads the kernel module.</td>
</tr>
</tbody>
</table>

### HTTPS Support for Configuration Download

For secure configuration download, Unified Communications Manager Release 11.0 is enhanced to support HTTPS in addition to the HTTP and TFTP interfaces that were used in the earlier releases. Both client and server use mutual authentication, if required. Clients that are enrolled with ECDSA LSCs and Encrypted TFTP configurations are required to present their LSC.

The HTTPS interface uses both the CallManager and the CallManager-ECDSA certificates as the server certificates.

---

**Note**

When you update CallManager, CallManager ECDSA, or Tomcat certificates, you must deactivate and reactivate the TFTP service. Port 6971 is used for authentication of the CallManager and CallManager-ECDSA certificates whereas port 6972 is used for the authentication of the Tomcat certificates.

---

### CTI Manager Support

The computer telephony integration (CTI) interface is enhanced to support four new ciphers. The ciphers suites are:

- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`,
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`,
- `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` and
- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`.

By supporting these cipher suites, the CTI Manager interface needs to have the CallManager-ECDSA certificate, if it exists in Unified Communications Manager. Similar to the SIP interface, the Enterprise Parameter `TLS Ciphers` option in Unified Communications Manager is used to configure the TLS ciphers that are supported on the CTI Manager secure interface.

### Generate Self-Signed Certificate

**Procedure**

1. **Step 1**
   - From Cisco Unified OS Administration, choose Security > Certificate Management.
   - The Certificate List window appears.

2. **Step 2**
   - Enter search parameters to find a certificate and view its configuration details.
   - The system displays the records that match all the criteria in the Certificate List window.

3. **Step 3**
   - Click Generate Self-Signed Certificate to generate a new self-signed certificate.
   - The Generate New Self-Signed Certificate window appears.

4. **Step 4**
   - From the Certificate Purpose drop-down box, select a system security certificate, such as CallManager-ECDSA.
**Step 5** Configure the fields in the **Generate New Self-Signed Certificate** window. See the Related Topics section for more information about the fields and their configuration options.

**Step 6** Click **Generate**.

---

**Related Topics**

[Self-signed Certificate Fields](#), on page 31

---

### Self-signed Certificate Fields

**Table 4: Self-signed Certificate Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Purpose</td>
<td>From the drop-down box, select a value:</td>
</tr>
<tr>
<td></td>
<td>• <strong>CallManager</strong>: When you select this option, the <strong>Key Type</strong> field is automatically set to <strong>RSA</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CallManager-ECDSA</strong>: When you select this option, the <strong>Key Type</strong> field is automatically set to <strong>EC</strong> (Elliptical Curve).</td>
</tr>
<tr>
<td>Distribution</td>
<td>Select a Unified Communications Manager server.</td>
</tr>
<tr>
<td>Common Name</td>
<td>Shows the name of the Unified Communications Manager application that you selected in the <strong>Distribution</strong> field.</td>
</tr>
<tr>
<td>Auto-populated Domains</td>
<td>This field appears in Subject Alternate Names (SANs) section and appears only for CallManager-ECDSA. The <strong>Auto-populated Domains</strong> field lists the host names that are to be protected by a single certificate. Generally, certificate common name is same as the host name. However, CallManager-ECDSA certificate has a common name that differs from host name. The <strong>Auto-populated Domains</strong> field displays the fully qualified domain name for CallManager-ECDSA certificate.</td>
</tr>
<tr>
<td>Key Type</td>
<td>This field lists the type of key used for encryption and decryption for the public-private key pair. Unified Communications Manager supports <strong>EC</strong> and <strong>RSA</strong> key types.</td>
</tr>
</tbody>
</table>
Generate Certificate Signing Request

If you generate a new certificate signing request for a specific certificate type, the application overwrites the existing certificate signing request for that certificate type.

**Generate Certificate Signing Request**

If you generate a new certificate signing request for a specific certificate type, the application overwrites the existing certificate signing request for that certificate type.

**Procedure**

**Step 1** From Cisco Unified OS Administration, choose Security > Certificate Management. The Certificate List window appears.

**Step 2** Click Generate CSR. The Generate Certificate Signing Request window appears.

**Step 3** Enter search parameters to find a certificate and view its configuration details. The system displays the records that match all the criteria in the Certificate List window.
Step 4  From the Certificate Purpose drop-down box, select a system security certificate, such as CallManager-ECDSA.

Step 5  Configure the fields in the Generate Certificate Signing Request window. See the Related Topics section for more information about the fields and their configuration options.

Step 6  Click Generate.

Related Topics
Certificate Signing Request Fields, on page 33

Certificate Signing Request Fields

Table 5: Certificate Signing Request Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Purpose</td>
<td>From the drop-down box, select a value:</td>
</tr>
<tr>
<td></td>
<td>• CallManager</td>
</tr>
<tr>
<td></td>
<td>• CallManager-ECDSA</td>
</tr>
<tr>
<td>Distribution</td>
<td>Select a Unified Communications Manager server.</td>
</tr>
<tr>
<td></td>
<td>When you select this field for multiserver for ECDSA, the syntax is:</td>
</tr>
<tr>
<td></td>
<td>Callmanager-ecdsa common name: &lt;host-name&gt;-EC-ms.&lt;domain&gt;</td>
</tr>
<tr>
<td></td>
<td>When you select this field for multiserver for RSA, the syntax is:</td>
</tr>
<tr>
<td></td>
<td>Callmanager common name: &lt;host-name&gt;-ms.&lt;domain&gt;</td>
</tr>
<tr>
<td>Common Name</td>
<td>Shows the name of the Unified Communications Manager application that you selected in the Distribution field by default.</td>
</tr>
<tr>
<td>Auto-populated Domains</td>
<td>This field appears in Subject Alternate Names (SANs) section. It lists the host names that are to be protected by a single certificate.</td>
</tr>
<tr>
<td>Parent Domain</td>
<td>This field appears in Subject Alternate Names (SANs) section. It shows the default domain name. You can modify the domain name, if required.</td>
</tr>
<tr>
<td>Key Type</td>
<td>This field identifies the type of key used for encryption and decryption for the public-private key pair.</td>
</tr>
<tr>
<td></td>
<td>Unified Communications Manager supports EC and RSA key types.</td>
</tr>
</tbody>
</table>
From the Key Length drop-down box, select one of the values. Depending on the key length, the CSR request limits the hash algorithm choices. By having the limited hash algorithm choices, you can use a hash algorithm strength that is greater than or equal to the key length strength. For example, for a key length of 256, the supported hash algorithms are SHA256, SHA384, or SHA512. Similarly, for the key length of 384, the supported hash algorithms are SHA384 or SHA512.

Certificates with a key length value of 3072 or 4096 can only be selected for RSA certificates. These options are not available for ECDSA certificates.

Some phone models may fail to register if the RSA key length selected for the CallManager Certificate Purpose is greater than 2048. From the Unified CM Phone Feature List Report on the Cisco Unified Reporting Tool (CURT), you can check the 3072/4096 RSA key size support feature for the list of supported phone models.

Select a value from the Hash Algorithm drop-down box to have stronger hash algorithm as the elliptical curve key length. From the Hash Algorithm drop-down box, select one of the values.

The values for the Hash Algorithm field change based on the value you select in the Key Length field.

If your system is running on FIPS mode, it's mandatory that you select SHA256 as the hashing algorithm.

**Upload Certificate or Certificate Chain**

Select and upload a certificate or a cluster-wide certificate to distribute it to all the servers in the selected cluster.

**Procedure**

**Step 1**

**Step 2**
Click Upload Certificate/Certificate chain.
The Upload Certificate/Certificate chain window appears.

**Step 3**
From the Certificate Purpose drop-down box, select a system security certificate, such as CallManager-ECDSA.

**Step 4**
In the Description field, enter a name for the certificate.

**Step 5**
In the Upload File field, click Choose File to browse for the certificate file that you want to distribute for all the servers in the cluster.
Interactions and Restrictions

- SIP devices that do not support `TLS_ECDHE_ECDSA_WITH_AES256_SHA384` and `TLS_ECDHE_ECDSA_WITH_AES128_SHA256` can still connect with `TLS_ECDHE_RSA_WITH_AES_256_SHA384`, `TLS_ECDHE_RSA_WITH_AES_128_SHA256`, or `AES128_SHA1`. These options are dependent on the TLS cipher option that you choose. If you choose **ECDSA only** option, then the device that does not support the ECDSA ciphers will not be able to make a TLS connection to the SIP interface. When you choose the **ECDSA only** option, the value of this parameter are `TLS_ECDHE_ECDSA_WITH_AES128_SHA256` and `TLS_ECDHE_ECDSA_WITH_AES256_SHA384`.

- CTI Manager Secure clients do not support `TLS_ECDHE_RSA_WITH_AES_128_SHA256`, `TLS_ECDHE_RSA_WITH_AES_256_SHA384`, `TLS_ECDHE_ECDSA_WITH_AES_128_SHA256`, and `TLS_ECDHE_ECDSA_WITH_AES_256_SHA384`. However, they can connect with `AES128_SHA1`.

Emergency Call Handler

Emergency Call Handler Overview

Emergency Call Handler helps you to manage emergency calls in your telephony network while following local ordinances and regulations.

When an emergency call is made the following is required:

- The emergency call must be routed to the local Public-Safety Answering Point (PSAP) based on the location of the caller.

- The caller's location information must be displayed at the emergency operator terminal. The location information can be obtained from an Automatic Location Information (ALI) database.

The caller's location is determined by the Emergency Location Identification Number (ELIN). An ELIN is a Direct Inward Dial (DID) number that the PSAP can dial to reconnect to the emergency caller if the emergency call is cut off or if the PSAP needs to talk to the caller again. The emergency call is routed to the PSAP based on the location information that is associated with this number.

For multiline phone systems, such as an office system, the ELIN can be associated with more than one telephone by grouping the phones in an ELIN group. An ELIN group in Emergency Call Handler identifies a location. The ELINs under this ELIN group must be mapped to the location in the ALI database.

Each location should have as many ELINs created as are needed to support simultaneous emergency calls. For example, to support five simultaneous calls five ELINs would be needed in an ELIN group.

Note

Emergency Call Handler supports a maximum of 100 ELIN groups per cluster.
The following types of phone are supported to use ELIN groups:

- SIP and SCCP IP phones
- CTI ports
- MGCP and SCCP analog phones
- H.323 phones

## Emergency Call Handler Prerequisites

### Example

Before deploying Emergency Call Handler in your network, we recommend that you test the ALI submission process. With your service provider’s help, test that the PSAP can successfully callback into your network using the ALI data.

Reserve the ELIN number from your local PSAP. Ordinances and regulations can differ across different locations and across different companies, so research your security and legal needs before deploying this feature.

## Emergency Call Handler Task Flow

### Before you begin

- Review Emergency Call Handler Prerequisites, on page 36

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enable Emergency Call Handler, on page 37</td>
<td>Enable the Emergency Call Handler feature on Cisco Unified Communications Manager. Emergency Call Handler provides essential emergency call features and supports a limited number of locations with phone location assignment by static configuration. If you require advanced emergency call features, such as a greater amount of specific locations or dynamic location assignment, consider Cisco Emergency Responder.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure Emergency Location Groups, on page 38</td>
<td>Configure an Emergency Location (ELIN) Group for a particular site or location.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Add a Device Pool to an Emergency Location Group, on page 39</td>
<td>Configure device pools to use an Emergency Location (ELIN) Group.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Add Device to an Emergency Location Group, on page 39</td>
<td>Configure a particular device to use a particular Emergency Location (ELIN) Group. If you want</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to use the device pool ELIN Group that is associated for this device, you can ignore this section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Configurations that are made at the device level will overwrite any configurations that were made at the device pool level.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**  
Enable Route Patterns and Translation Patterns, on page 40  
Enable the Emergency Location (ELIN) service for a route pattern or a translation pattern.  
**Caution** No Calling Party Transformation masks are set at the Gateway or Trunk, because these may transform the ELIN that is set by Emergency Call Handler.  
**Note** It is mandatory that you enable either route patterns or translation patterns, but it is possible to enable both.

**Step 6**  
(Optional) Use the following procedures to perform bulk administration tasks on ELIN group information and phones:  
- Import Emergency Location Group Information, on page 41  
- Export Emergency Location Group Information, on page 42  
- Update Phones with a new Emergency Location Group, on page 42  
This section provides information about the Bulk Administration tasks you can use to update ELIN group information and to add phones to new ELIN groups. For Bulk Administration, see the *Cisco Unified Communications Manager Bulk Administration Guide, Release 11.0(1)*.

---

**Enable Emergency Call Handler**

Enable the Emergency Call Handler feature on Cisco Unified Communications Manager. Emergency Call Handler provides essential emergency call features and supports a limited number of locations with phone location assignment by static configuration. If you require advanced emergency call features, such as a greater amount of specific locations or dynamic location assignment, consider Cisco Emergency Responder.

**Note** Do not enable this feature if you are already using an external emergency calling solution such as Cisco Emergency Responder.

If you decide to enable this feature, make sure you disable the external one.
Configure Emergency Location Groups

Configure an Emergency Location (ELIN) Group for a particular site or location.

Before you begin

Enable Emergency Call Handler, on page 37

Procedure

Step 1 From Cisco Unified CM Administration, choose Call Routing > Emergency Call Handler > Emergency Location (ELIN) Group.

Step 2 In the Emergency Location (ELIN) Group Configuration window, enter a name for the group in the Name field.

Step 3 In the Number field, enter the pool of DID numbers that are registered in the Public Safety Answering Point (PSAP).

Step 4 Click Save.
Add a Device Pool to an Emergency Location Group

Configure device pools to use an Emergency Location (ELIN) Group.

Before you begin
Configure Emergency Location Groups, on page 38

Procedure

Step 1  From Cisco Unified CM Administration, choose System > Device Pool.
Step 2  In the Find and List Device Pools window, if you are adding an existing device pool, click Find and choose the device pool from the list. If you are adding a new device pool click Add New.
Step 3  In the Device Pool Configuration window, choose the ELIN group to which you want to add the device pool from the Emergency Location (ELIN) Group drop-down list. If you are adding a new device pool, fill out any other required fields.
Step 4  Click Save.

What to do next
Add Device to an Emergency Location Group, on page 39

Add Device to an Emergency Location Group

Configure a particular device to use a particular Emergency Location (ELIN) Group. If you want to use the device pool ELIN Group that is associated for this device, you can ignore this section.

Note
Configurations that are made at the device level will overwrite any configurations that were made at the device pool level.

Note
The devices that you add to the ELIN Group, should be added to the ELIN Group that represents the particular location at which those devices are located.

Before you begin
Add a Device Pool to an Emergency Location Group, on page 39
Procedure

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

Note  If you are using a type of phone that is not an IP phone, go to the relevant configuration page for that type of phone.

Step 2  In the Find and List Phones window, if you are adding an existing device, click Find and choose the device you want to configure from the list. If you are adding a new device, click Add New.

Step 3  If you are adding a new phone, choose the type of phone you want to add from the Phone Type drop-down list and click Next.

Step 4  In the Phone Configuration window, choose the ELIN group to which you want to add the device from the Emergency Location (ELIN) Group drop-down list. If you are adding a new device, fill out any other required fields.

Step 5  Click Save.

What to do next
Enable Route Patterns and Translation Patterns, on page 40

Enable Route Patterns and Translation Patterns

Enable the Emergency Location (ELIN) service for a route pattern or a translation pattern.

Note  It is mandatory that you enable either route patterns or translation patterns, but it is possible to enable both.

Before you begin
Add Device to an Emergency Location Group, on page 39

Procedure

Step 1  From Cisco Unified CM Administration, choose one of the following:

- To enable a route pattern, choose Call Routing > Route/Hunt > Route Pattern.
- To enable a translation pattern, choose Call Routing > Translation Pattern.

Step 2  In the Find and List Route Patterns or Find and List Translation Patterns window, click Find and choose a route pattern or translation pattern from the list.

Step 3  In the Route Pattern Configuration or Translation Pattern Configuration window, check the Is an Emergency Services Number check box.

Note  Check this check box only if you are using Emergency Call Handler and not another external emergency calling solution such as Cisco Emergency Responder.

Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.0(1)
Bulk Administration of Emergency Location Groups and Phones

• Bulk Administration of Emergency Location Groups and Phones Task Flow, on page 41

Bulk Administration of Emergency Location Groups and Phones Task Flow

This section provides information about the Bulk Administration tasks you can use to update ELIN group information and to add phones to new ELIN groups. For more information about Bulk Administration, see the Cisco Unified Communications Manager Bulk Administration Guide, Release 11.0(1).

Note

Before you perform these procedures, make sure that you have enable the Emergency Call Handler feature. See Enable Emergency Call Handler, on page 37.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Import Emergency Location Group Information, on page 41</td>
<td>Import Emergency Location (ELIN) Group information using the Bulk Administration Tool.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Export Emergency Location Group Information, on page 42</td>
<td>Export Emergency Location (ELIN) Group information using the Bulk Administration Tool.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Update Phones with a new Emergency Location Group, on page 42</td>
<td>Find and list multiple phones and configure them with a new Emergency Location (ELIN) Group.</td>
</tr>
</tbody>
</table>

Import Emergency Location Group Information

Import Emergency Location (ELIN) Group information using the Bulk Administration Tool.

Procedure

Step 1 From Cisco Unified CM Administration, choose Bulk Administration > Import/Export > Import.
Step 2 From the File Name drop-down list, choose the name of the .tar file you want to import, and click Next.
Step 3 The Import Configuration section lists all the components of the .tar file. Check the ELIN Group-related check boxes for the options that you want to import.
Step 4 Choose to run the job immediately or later by clicking the corresponding radio button.
Step 5 To create a job for importing the selected data, click Submit. A message in the Status section notifies you know that the job was submitted successfully.
Step 6 Use the Job Scheduler option in the Bulk Administration main menu to schedule or activate this job.
What to do next

Export Emergency Location Group Information, on page 42

Export Emergency Location Group Information

Export Emergency Location (ELIN) Group information using the Bulk Administration Tool.

Before you begin

Import Emergency Location Group Information, on page 41

Procedure

Step 1  From Cisco Unified CM Administration, choose Bulk Administration > Import/Export > Export.

Step 2  In the Export Data window, in the Job Information pane, enter the .tar file name, without the extension, in the Tar File Name field. BPS uses this filename to export the configuration details.

Note  All files that are exported at the same time get bundled together (.tar) and can be downloaded from the server.

Step 3  To export ELIN Group information, check the Elin Group check box on the Select items to Export pane.

Step 4  (Optional) Perform these steps:

• To export device pools with ELIN Groups configured, check the Device Pools check box.
• To export phones with ELIN Groups configured, check the Phone check box.

Step 5  In the Job Description field, enter the description that you want to override for the job. Export Configuration is the default description.

Step 6  You can choose to run the job immediately or later by clicking the corresponding radio button.

Step 7  To create a job for exporting the selected data, click Submit. A message in the Status pane notifies you that the job was submitted successfully.

Step 8  Use the Job Scheduler option in the Bulk Administration main menu to schedule or activate this job.

What to do next

Update Phones with a new Emergency Location Group, on page 42

Update Phones with a new Emergency Location Group

Find and list multiple phones and configure them with a new Emergency Location (ELIN) Group.

Before you begin

Export Emergency Location Group Information, on page 42

Procedure

Step 1  From Cisco Unified CM Administration, choose Bulk Administration > Phones > Update Phone > Query.
Step 2  In the Find and List Phones To Update window, set the parameters for your search and click Find.

**Note**  To update all phones, click Find and do not specify a query.

Step 3  The Find and List Phones To Update window displays the details of the phones that you chose. Click Next.

Step 4  In the Update Phones window, check the Emergency Location (ELIN) Group check box, and choose a new ELIN Group from the drop-down list.

Step 5  Click Submit.

---

**Emergency Call Handler Interactions and Restrictions**

- **Interactions,** on page 43
- **Restrictions:** None

**Interactions**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction</th>
</tr>
</thead>
</table>
| Do Not Disturb Call Reject | Calls made by PSAP CallBack will overwrite a Do Not Disturb (DND) configuration of a destination device.  
If DND Call Reject is enabled, when the emergency number is dialed using the translation pattern, an ELIN will be associated for this outbound emergency call.  
If the call is disconnected and the ELIN is called back using PSAP CallBack, the call is routed to the phone irrespective of the phone's DND settings. |
| Call Forward All | Calls made by PSAP CallBack will overwrite Call Forward All (CFA) settings of the destination device.  
If a phone has CFA enabled and if the emergency number using the translation pattern is dialed, an ELIN will be associated for this outbound emergency call.  
If the call is disconnected and the ELIN is called back using PSAP CallBack, the call is routed to the phone irrespective of the phone's CFA settings. |
| Single Number Reach | PSAP CallBack will ignore the Single Number Reach (SNR) configuration.  
When a phone has SNR enabled with the Remote Destination pointing to a mobile number. If the emergency number is dialed using the translation pattern, an ELIN will be associated for this outbound emergency call.  
If the call is disconnected, and the ELIN number is called back using PSAP CallBack, the call is routed to the phone and not to the remote destination. |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction</th>
</tr>
</thead>
</table>
| Extension Mobility | PSAP CallBack call will consider Extension Mobility (EM) status.  
If you log in with EM profile credentials and dial the emergency number using the translation pattern, an ELIN will be associated for this outbound emergency call. If the call is disconnected and the ELIN where the user is still logged in is called back using PSAP CallBack, the call is routed to the device which initiated the call.  
**Note** This is the device on which the user is still logged in. |
|              | PSAP CallBack will fail if a user logs out of EM before a PSAP CallBack is performed.  
When a user logs in with EM profile credentials, and the emergency number is dialed using the translation pattern, an ELIN will be associated for this outbound emergency call. If the call is disconnected and is called back using PSAP CallBack, if the user has since logged out, the call will not route to the device that initiated the call and will fail. |
|              | PSAP CallBack with a user logged in on a different device.  
When a user logs in with EM profile credentials at Phone A and dials the emergency number using the translation pattern, an ELIN will be associated for this outbound emergency call. If the call is disconnected, the user should log out from Phone A. If the user then logs in to another phone, Phone B, with the same profile, and the ELIN is called back using PSAP CallBack, the call is then be routed to Phone B with normal priority, meaning CFA settings will be ignored and DND settings will not be ignored. |
|              | PSAP CallBack call with multiple logins.  
When a user logs in with EM profile credentials at Phone A and dials the emergency number using the translation pattern, an ELIN number will be associated for this outbound emergency call. If the call is disconnected and the user logs in to another phone, Phone B, with the same profile while the user is still logged in on Phone A, and the ELIN is called back using PSAP CallBack, then the call is routed to Phone A only, the device on which the call originated. |
| Device Mobility | A roaming device will use the Roaming Device Pool's ELIN Group for an outbound emergency call.  
Move a device with Device Mobility enabled from its home location to the Roaming location, a change in IP subnet, so that it gets associated with the Roaming device pool. If the emergency number is dialed using the translation pattern, an ELIN is associated for this outbound emergency call. The ELIN belongs to the ELIN Group that is associated with the Roaming Device Pool. |
### Emergency Call Handler Troubleshooting

**About Emergency Call Handler Troubleshooting Scenarios**

This section provides information about some Emergency Call Handler troubleshooting scenarios in the following areas:

- Configuration Scenarios
- Outgoing Calls Scenarios
- Incoming Calls Scenarios

### Configuration Scenarios

**Emergency Calls Get Busy Signals and Are Not Routed**

**Problem:**

Emergency calls get busy signals and are not routed.

**Solution:**

If a user who is dialing the emergency call is running a reorder tone, perform the following checks:

- Check whether the translation or route pattern for the emergency call has been used. This may require checking for the device or phone on CSS.
- Check whether the **Is an Emergency Services Number** checkbox has been checked for the translation or route pattern of the emergency call, and that it is correctly routing to the gateway.

If the user who is dialing the emergency call is not reaching the correct gateway or Public Service Answering Point (PSAP), check that the settings or device pool settings for the phone or device are configured with the correct Emergency Location (ELIN) Group.

**Emergency Location Numbers Are Dialed from Outside Running a Reorder Tone**

**Problem:**

Emergency Location (ELIN) numbers are dialed from outside while running a reorder tone.

**Cause:**

In this case the ELINs have been set as DID which is used to identify a caller's location. This should not be used on any phone or for any other purpose.
Outgoing Calls Scenarios

**Outgoing Emergency Call Does Not Contain Calling Party as Emergency Location Number**

**Problem:**
An outgoing emergency call does not contain the calling party as an Emergency Location (ELIN) number.

**Cause:**
The translation pattern or route pattern for this ELIN was not configured correctly.

**Solution:**
Check that the translation pattern or route pattern settings are correctly configured for this ELIN, and make sure that the **Is an Emergency Services number** check box is checked on the relevant translation pattern or route pattern configuration page.

**Outgoing Emergency Call Contains Modified Emergency Location Number**

**Problem:**
An outgoing emergency call contains a modified Emergency Location (ELIN) number.

**Cause:**
The outgoing trunk or route list contains extra transformations that are not required for ELINs.

**Solution:**
Check the transformations that were applied for the call, and make sure that only the required transformations for ELINs are present on the outgoing trunk or route list.

Incoming Calls Scenarios

**Incoming PSAP Callback Call Fails**

**Problem:**
An incoming PSAP Callback call fails.

**Cause:**
The device that made the original emergency call was not registered correctly.

**Solution:**
Check whether the device that made the original emergency call is still registered and whether any Extension Mobility is involved.

**Incoming PSAP CallBack Call is Not Routed as Expected**

**Problem:**
An incoming PSAP CallBack call does not get routed as expected.

**Cause:**
The Emergency Location (ELIN) number does not match the number of the original dialed party.
Solution:
For an ELIN to be successfully reverse mapped to the original dialed party, these two numbers must match. If there are already transformations at the incoming Gateway or Trunk and significant digits configured, make sure that the final transformed called party matches the ELIN number.

Quality of Service Updates

For Release 11.0(1) of Cisco Unified Communications Manager, the following Quality of Service (QoS) updates were made:

- **Quality of Service (QoS) with APIC-EM Controller, on page 47**—As of Release 11.0(1), you can now assign an APIC-EM Controller to dynamically manage network traffic and set the priority for specific media packet types in order to relieve congested networks and ensure QoS.

- **Custom QoS Settings for Users, on page 49**—DSCP configuration has been enhanced for Release 11.0(1). In previous releases, DSCP settings for the users in your network were configured using service parameters, and the same settings were applied to all users in the network. With Release 11.0(1), you can now customize DSCP settings within a SIP Profile and then associate that SIP profile to a device. You can also configure separate port ranges for the audio and video streams in order to dedicate ports to one media type and simplify network bandwidth management.

- **Call Admission Control Enhancement for Audio Portion of Video Calls, on page 53**—In Release 11.0(1), the Call Admission Control (CAC) feature has been enhanced for video calls. For video calls, CAC can now be configured to split the bandwidth deductions for the audio stream and the video stream into separate pools. If this feature is configured, the bandwidth that is required for the IP/UDP network overhead is also deducted from the audio pool.

Quality of Service (QoS) with APIC-EM Controller

In order to manage network Quality of Service (QoS) for SIP calls, you can deploy a Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM). APIC-EM applies DSCP markings to media flows that are created by communication sessions among Cisco Unified Communications Manager-managed SIP endpoints and trunks. Applying DSCP markings to media flows ensures that audio and video media will not be blocked by other lower-priority network traffic such as email, print jobs, and software downloads. The APIC-EM assigns DSCP markings on a per-call basis for audio and video packets according to the priority assigned to the endpoint by Cisco Unified Communications Manager. The DSCP values that are assigned by the APIC-EM override any DSCP values that are set by an endpoint.

The following call example demonstrates how the APIC-EM manages QoS for SIP calls:

1. During the call setup, Cisco Unified Communications Manager signals to the APIC-EM the following information for each media flow:
   1. Source and destination IP address and port for the media flow.
   2. Priority setting for the media flow as determined by the endpoint type in Cisco Unified Communications Manager (for example, TelePresence).
   3. The media type (for example, audio or video).

2. The APIC-EM determines the switch ports where the identified endpoints attach to the network.
3. The APIC-EM maps the priority sent by Cisco Unified Communications Manager to a specific DSCP value.

4. The APIC-EM sends the DSCP values for the media types involved in the call to the access switch where the flow enters the network.

5. The access switch marks each packet in the flow with the specified DSCP values.

6. When the call ends, Cisco Unified Communications Manager signals the APIC-EM that the flow can be deleted.

7. APIC-EM notifies the switches where the media flow enters the network to stop marking the flows.

**APIC-EM Controller Configuration**


**GUI Changes for APIC-EM Controller**

The **HTTP Profile** window has been updated for Release 11.0(1). The following table shows the fields in the HTTP Profile window.

*Table 6: HTTP Profile Settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the HTTP Profile. For example, if you are connecting to an APIC-EM controller for network traffic management, you could enter a name such as 'APIC-EM Service'.</td>
</tr>
<tr>
<td>Web Service Root URI</td>
<td>Enter an IP address or fully qualified domain name for the external web service to which you want to connect.</td>
</tr>
</tbody>
</table>

The following fields, which were included in the previous release of Cisco Unified Communications Manager, have been removed from the **HTTP Profile** window:

- User Name
- Password
- Request Timer
- QoS Connection Type
- QoS URI
Custom QoS Settings for Users

With Release 11.0(1), you can customize Quality of Service (QoS) settings within a SIP profile and apply those settings to your users. The SIP Profile Configuration window has been enhanced with the following types of QoS settings:

- Custom DSCP values for audio and video streams
- Custom UDP port ranges for audio and video streams

Custom DSCP Values for Audio and Video

You can configure DSCP values for audio and video calls within a SIP profile and apply them to the SIP phones that use that profile. The SIP Profile Configuration window includes custom DSCP settings for the following types of calls:

- Audio calls
- Video calls
- Audio portion of a video call
- TelePresence calls
- Audio portion of a TelePresence call

If your company has a set of employees, such as a sales force, or a CEO, who require higher QoS priority settings than the majority of your employees, you can use the SIP profile configurations to configure custom DSCP values for those users. The settings within the SIP profile override the corresponding clusterwide service parameter settings.

Custom UDP Port Ranges for Audio and Video

You can configure separate UDP port ranges for the audio stream and video stream of a SIP call. Because video typically requires considerably more bandwidth than audio, creating dedicated port ranges for each media type simplifies network bandwidth management. It also protects against audio stream degradation by guaranteeing that the audio stream will have a dedicated channel that is separate from the higher-bandwidth video stream.

You can apply this configuration by setting the Media Port Ranges field in the SIP profile to Separate Port Ranges for Audio and Video. You can then apply the configuration to a phone by associating the SIP profile to a phone.

Configure Custom QoS Policy for Users

Perform the following tasks to set up a custom Quality of Service (QoS) policy for users. You may want to apply a custom policy if a set of users within your company has different QoS requirements from the rest of the company. For example, a telephone sales force or a CEO.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Configure Custom QoS Settings in SIP Profile, on page 50</strong></td>
<td>Configure a SIP Profile with customized DSCP values and a UDP port range for audio and video streams.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Apply Custom QoS Policy to a Phone, on page 51</strong></td>
<td>Apply the SIP Profile to a phone. The DSCP settings in the SIP Profile override the DSCP clusterwide service parameter settings.</td>
</tr>
</tbody>
</table>

### Configure Custom QoS Settings in SIP Profile

Configure custom DSCP values and UDP port ranges for the phones that use this SIP Profile. You can use these settings to configure a customized QoS policy that you can apply to specific phones and users within your network. You may want to do this if you want to apply specific QoS settings to specific users within your enterprise, such as a sales force, or a CEO.

**Procedure**

1. From Cisco Unified CM Administration, choose **Device > Device Settings > SIP Profile**.
2. Perform either of the following steps:
   - Click **Find** and select an existing SIP Profile.
   - Click **Add New** to create a new SIP Profile.
3. From the **Media Port Ranges** field, select whether you want to assign a single UDP port range that handles both audio and video media, or separate port ranges for audio and video streams.
   - If you want to configure a single port range for audio and video media, enter the range of ports in the **Start Media Port** and **Stop Media Port** fields. The possible port values are between 2048 and 65535.
   - If you want separate port ranges for audio and video streams, enter the range of audio ports using the **Start Audio Port** and **Stop Audio Port** fields. Enter the range of video ports using the **Start Video Port** and **Stop Video Port** fields. The possible port values for each are between 2048 and 65535. The two port ranges must not overlap.
4. In the following fields, configure customized DSCP values for audio and video streams.
   - **DSCP for Audio Calls**
   - **DSCP for Video Calls**
   - **DSCP for Audio Portion of Video Calls**
   - **DSCP for TelePresence Calls**
   - **DSCP for Audio Portion of TelePresence Calls**

   **Note** By default, each of the above fields is configured to use the value from a corresponding service parameter. If you assign new values, the new value overrides the service parameter setting.
5. Complete the remaining fields in the **SIP Profile Configuration** window. For help with the fields and their settings, refer to the online help.
6. Click **Save**.
Apply Custom QoS Policy to a Phone

Use this procedure to apply a SIP Profile that contains customized QoS settings, including DSCP values and a UDP port range for audio and video media. When you apply this SIP profile to a phone, the phone uses the custom settings from the SIP Profile.

Before you begin

Configure Custom QoS Settings in SIP Profile, on page 50

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From Cisco Unified CM Administration, choose Device &gt; Phone.</td>
</tr>
</tbody>
</table>
| Step 2 | Perform either of the following steps:  
|  | • Click Find and select an existing phone.  
|  | • Click Add New to create a new phone. |
| Step 3 | From the SIP Profile drop-down list, select the SIP profile that you set up with the custom DSCP values and UDP port range values. |
| Step 4 | Complete the remaining fields in the Phone Configuration window. For help with the fields and their settings, refer to the online help. |
| Step 5 | Click Save. |

GUI Changes for Custom QoS Settings

The SIP Profile Configuration window has been updated with the following new fields:

• Media Port Ranges
• Start Audio Port
• Stop Audio Port
• Start Video Port
• Stop Video Port
• DSCP for Audio Calls
• DSCP for Video Calls
• DSCP for Audio Portion of Video Calls
• DSCP for TelePresence Calls
• DSCP for Audio Portion of TelePresence Calls

The following table displays field descriptions for the new fields.
Table 7: New Fields for the SIP Profile Configuration Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Port Ranges</td>
<td>Click the radio button that corresponds to how you want to manage QoS for audio and video calls for devices that are associated to this SIP Profile:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Common Port Range for Audio and Video</strong>—Choose this option if you want to use a single port range for both the audio and video media stream.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Separate Port Range for Audio and Video</strong>—Choose this option if you want to set up a distinct port range for the audio stream and a distinct port range for the video stream.</td>
</tr>
<tr>
<td>Start Audio Port</td>
<td>Create a port range for audio by entering the start of the port range. The available values range from 2048 to 65535. You can configure an audio port range only if you select <strong>Separate Port Ranges for Audio and Video</strong> for the Media Port Range.</td>
</tr>
<tr>
<td>Stop Audio Port</td>
<td>Enter the ending of the port range for audio calls.</td>
</tr>
<tr>
<td>Start Video Port</td>
<td>Create a port range for the video stream of a video call by entering the beginning of the port range. The available values range from 2048 to 65535. The audio port range and video port ranges cannot overlap. You can only configure a video port range only if you select <strong>Separate Port Ranges for Audio and Video</strong> for the Media Port Range.</td>
</tr>
<tr>
<td>Stop Video Port</td>
<td>Enter the ending of the port range for audio calls.</td>
</tr>
<tr>
<td>DSCP for Audio Calls</td>
<td>Select the value that you want to assign as the DSCP value for audio-only calls. The Default Option is to use the value of the DSCP for Audio Calls service parameter.</td>
</tr>
<tr>
<td>DSCP for Video Calls</td>
<td>Select the value that you want to assign as the DSCP value for video calls. The Default Option is to use the value of the DSCP for Video Calls service parameter.</td>
</tr>
<tr>
<td>DSCP for Audio Portion of Video Calls</td>
<td>Select the value that you want to assign as the DSCP value for audio portion of a video call. The default option is to use the value that is configured in the DSCP for Audio Portion of Video Calls service parameter.</td>
</tr>
<tr>
<td>Note</td>
<td>If you choose a different DSCP value for the audio portion of video calls than you configured for video calls, the audio and video streams within a single video call could have different DSCP markings and different QoS policy control. This could result in lip sync issues that result from network bandwidth issues.</td>
</tr>
</tbody>
</table>
Call Admission Control Enhancement for Audio Portion of Video Calls

With Release 11.0(1), the Call Admission Control (CAC) feature has been enhanced for video calls. You can now configure CAC to split the audio and video bandwidth deductions for video calls into separate pools. When this feature is enabled, CAC deducts the bandwidth required for the audio stream of a video call from the audio pool and the bandwidth required for the video stream from the video pool.

To configure this option, enable the Deduct Audio Bandwidth from Audio Pool for Video Calls service parameter. The possible values for this service parameter are True or False:

- **True**—For video calls, the system deducts the bandwidth required for the audio stream from the audio pool and the bandwidth required for the video stream from the video pool. The audio bandwidth deduction includes audio bitrate plus the IP/UDP network overhead. The video pool deduction includes the video bit rate only.

- **False**—This is the default setting. For video calls, the system deducts the bandwidth for both the audio and video streams from the video pool. This deduction includes both the audio and video bit rates. Any bandwidth required for the IP/UDP overhead is ignored.

When you enable this feature, CAC includes the bandwidth that is required for the IP/UDP network overhead in the audio bandwidth deduction, which is the audio bitrate plus the IP/UDP network overhead bandwidth requirement. The video bandwidth deduction is the video bit rate only.

**Deduct Audio Bandwidth from Audio Pool for Video Calls**

Use this procedure if you want to split the audio and video bandwidth deductions into separate pools for video calls. By default, the system deducts the bandwidth requirement for both the audio stream and video stream from the video pool for video calls.

When you enable this feature, CAC includes the bandwidth required for the IP/UDP network overhead in the audio bandwidth deduction. This audio bandwidth deduction equates to the audio bitrate plus the IP/UDP network overhead bandwidth requirement. The video bandwidth deduction is the video bit rate only.

**Table:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP for TelePresence Calls</td>
<td>Select the value that you want to assign as the DSCP value for TelePresence calls. The default option is to use the value of the DSCP for TelePresence Calls service parameter.</td>
</tr>
</tbody>
</table>

**Call Admission Control Enhancement for Audio Portion of Video Calls**

Call Admission Control Enhancement for Audio Portion of Video Calls

With Release 11.0(1), the Call Admission Control (CAC) feature has been enhanced for video calls. You can now configure CAC to split the audio and video bandwidth deductions for video calls into separate pools. When this feature is enabled, CAC deducts the bandwidth required for the audio stream of a video call from the audio pool and the bandwidth required for the video stream from the video pool.

To configure this option, enable the Deduct Audio Bandwidth from Audio Pool for Video Calls service parameter. The possible values for this service parameter are True or False:

- **True**—For video calls, the system deducts the bandwidth required for the audio stream from the audio pool and the bandwidth required for the video stream from the video pool. The audio bandwidth deduction includes audio bitrate plus the IP/UDP network overhead. The video pool deduction includes the video bit rate only.

- **False**—This is the default setting. For video calls, the system deducts the bandwidth for both the audio and video streams from the video pool. This deduction includes both the audio and video bit rates. Any bandwidth required for the IP/UDP overhead is ignored.

When you enable this feature, CAC includes the bandwidth that is required for the IP/UDP network overhead in the audio bandwidth deduction, which is the audio bitrate plus the IP/UDP network overhead bandwidth requirement. The video bandwidth deduction is the video bit rate only.

**Deduct Audio Bandwidth from Audio Pool for Video Calls**

Use this procedure if you want to split the audio and video bandwidth deductions into separate pools for video calls. By default, the system deducts the bandwidth requirement for both the audio stream and video stream from the video pool for video calls.

When you enable this feature, CAC includes the bandwidth required for the IP/UDP network overhead in the audio bandwidth deduction. This audio bandwidth deduction equates to the audio bitrate plus the IP/UDP network overhead bandwidth requirement. The video bandwidth deduction is the video bit rate only.
Procedure

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

Step 2  From the **Server** drop-down list, choose the publisher node.

Step 3  From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4  From the **Clusterwide Parameters (Call Admission Control)** area, set the value of the **Deduct Audio Bandwidth Portion from Audio Pool for a Video Call** service parameter to **True**.

Step 5  Click **Save**.

Removal of End-to-End RSVP Support

Starting with Release 11.0(1), you can no longer configure End-to-End RSVP functionality within the SIP Profile page.

Location-based service on Cisco Emergency Responder

The Location-Based service on Cisco Emergency Responder (CER) feature enables Cisco Unified Communications Manager to learn infrastructure elements, receive upstream neighbor information from Wired and Wireless Endpoints, process and format the information, then send the update to the Database for storage.

For Release 11.0(1) of Cisco Unified Communications Manager, the following updates have been made:

- Infrastructure Device Setup using Bulk Administration Tool.
- CSV Data Files Creation for Infrastructure Devices Using Text Editor.

Cisco Unified Communications Manager cache responses to A/AAAA queries

The following sections describe the trouble shooting steps added as part of Cisco Unified Communications Manager Release 11.0(1).

Logging

**Symptom**

Set debug level for logging.

**Recommended Action**

Set network name-service debug-level 3(default 0)

- level 0 - no logging
• level 1 – errors, some cache removals
• level 2 – cache population
• level 3 and greater – entries considered for cache hits, pruning cache

Log file

Log file: activelog syslog/nscd.log

Consider the following example for Sample log file content:

Wed Dec 17 18:26:01 2014 - 21908: Have not found "clock.cisco.com" in hosts cache!
Wed Dec 17 18:26:01 2014 - 21908: add new entry "clock.cisco.com" of type GETHOSTBYNAME for hosts to cache (first)
Wed Dec 17 18:26:01 2014 - 21908: handle_request: request received (Version = 2) from PID 22151

Packet Capture

utils network capture port 53

Example:

admin: utils network capture port 53

Executing command with options:

size=128 count=1000 interface=eth0

A/AAAA record caching is not working

Symptom

A/AAAA record caching is not working. An A/AAAA record query is sent every time SIP call needs host name resolution.

Corrective Action

Check the status of Name Service Cache service. The status should be “Started” as given below:
Hostname resolution returning wrong IP address

Symptom
Hostname resolution returns a wrong IP address.

Possible Cause
The cache is obsolete. This is usually due to A/AAAA record changes in DNS server.

Corrective Action
• Flush the current cache using the following CLI command:

admin:utils network name-service hosts cache invalidate

  • If problem persists, restart nscd using the following CLI command:

admin:utils service restart Name Service Cache

  • If problem still persists, disable nscd using the following CLI command:

admin: utils service stop Name Service Cache
• If problem still persists check the A/AAAA record configuration in the DNS server.

Cannot find log

Symptom
Cannot find log /var/log/active/syslog/nscd.log

Corrective Action
Check that the debug level is above 0 (default is 0). After updating debug level, restart nscd using the following CLI command:

```
admin:utils service restart Name Service Cache
```

Set nscd attributes through CLI

Symptom
I set nscd attributes via CLI, but the new attribute values are not taking effect.

Corrective Action
Restart nscd after any attribute change, using the following CLI command:

```
utils service restart Name Service Cache
```

CLI command to set TTL

Symptom
I used CLI command to set TTL for the nscd cache entries, but the value I set is not taking effect for A/AAAA record cache.

Corrective Action
The TTL configured for the A/AAAA record on the DNS server will override the configuration set for nscd. The TTL configured for nscd will take effect only if TTL is not configured for the A/AAAA record on DNS server.

A/AAAA Record Queries before TTL expires

Symptom
Name Service Cache is enabled, I still see multiple A/AAAA record Queries sent to DNS Server before TTL expires.
Corrective Action
These queries are most likely triggered by nscd reloading the existing cache entries. Nscd reloading behavior is related to the reload-count in the nscd configuration file.

Clearing the cache

Symptom
Will restarting nscd clear the A/AAAA record cache?

Corrective Action
Restarting nscd does not always clear/flush the cache. It depends on the persistent attribute configuration.

• If the persistent attribute is set to Yes, the cache remains the same when nscd restarts.
• If the persistent attribute is set to No (default), the cache will be cleared/flushed when nscd restarts.

To clear/flush the cache, use the following CLI command:
admin:utils network name-service hosts cache invalidate

Content of AAAA record cache

Symptom
Can I see the content of A/AAAA record cache?

Corrective Action
No. NSCD activities can only be observed in nscd.log (with desired debugging level setting). A/AAAA record caching statistics can also be queried using the CLI command:
admin:show network name-service hosts cache-stats

CLI Commands for DNS Caching

The following CLI Commands have been added for Cisco Unified Communications Manager Release 11.0.

show network name-service attributes
This command displays name service cache general attributes.

Command Modes
Administrator (admin:)

Requirements
Command privilege level: 1
Allowed during upgrade: No
Example:

```
admin:show network name-service hosts attributes
enable-cache yes
positive-time-to-live 3600
negative-time-to-live 20
```

Successful

**show network name-service cache-stats**

This command displays name service cache statistics.

```
show network name-services[host][services] cache-stats
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>host services cache.</td>
</tr>
<tr>
<td>services</td>
<td>services service cache.</td>
</tr>
</tbody>
</table>

### Command Modes

Administrator (admin:)

### Requirements

Command privilege level: 1  
Allowed during upgrade: No

Example:

```
admin:show network name-service hosts cache-stats
yes cache is enabled
   no cache is persistent
   yes cache is shared
   211 suggested size
216064 total data pool size
   272 used data pool size
   3600 seconds time to live for positive entries
   20 seconds time to live for negative entries
   0 cache hits on positive entries
   0 cache hits on negative entries
   2 cache misses on positive entries
   0 cache misses on negative entries
   0% cache hit rate
   2 current number of cached values
   2 maximum number of cached values
   0 maximum chain length searched
   0 number of delays on rdlock
   0 number of delays on wrlock
   0 memory allocations failed
yes check /etc/hosts for changes
```

Successful
show network name-service {hosts|services} attributes

This command displays name service cache attributes.

Syntax Description

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>hosts services cache.</td>
</tr>
<tr>
<td>services</td>
<td>services service cache.</td>
</tr>
</tbody>
</table>

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Example:

```
admin:show network name-service hosts attributes
enable-cache yes
positive-time-to-live 3600
negative-time-to-live 20
suggested-size 211
persistent no
max-db-size 33554432
```

set network name-service

This command displays name service cache attributes.

Syntax Description

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paranoia</td>
<td>Bool must be either Yes or No. Enabling paranoia mode causes Name Service to restart itself periodically.</td>
</tr>
<tr>
<td>debug-level</td>
<td>If level is higher than 0, Name Service will create some debug output. Higher the level, more verbose the output.</td>
</tr>
<tr>
<td>reload-count</td>
<td>Sets the number of times a cached record is reloaded before it is pruned from the cache. Each cache record has a timeout. When that timeout expires Name Service will either reload it (query the NSS service again if the data hasn't changed) or drop it.</td>
</tr>
<tr>
<td>restart-interval</td>
<td>Sets the restart interval to time seconds if periodic restart is enabled by enabling paranoia mode. The default value is 3600.</td>
</tr>
</tbody>
</table>
**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1
Allowed during upgrade: No

### set network name-service hosts services

This command displays name service cache attributes

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>host services cache.</td>
</tr>
<tr>
<td>services</td>
<td>services service cache.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable-cache</td>
<td>Bool must be either Yes or No. Each cache is disabled by default and, must be enabled explicitly by setting this option to Yes.</td>
</tr>
<tr>
<td>Positive-time-to-live</td>
<td>Number-of-seconds. This is the number of seconds after which a cached entry is removed from the cache when DNS is not configured with TTL values. This defaults to 3600 seconds (i.e. one hour).</td>
</tr>
<tr>
<td>Negative-time-to-live</td>
<td>Number-of-seconds. If an entry is not found by the Name Service, it is added to the cache and marked as &quot;not existent&quot;. This option sets the number of seconds after which, such a non existent entry is removed from the cache. This defaults to 20 seconds.</td>
</tr>
<tr>
<td>Suggested-size</td>
<td>Number of bytes. Sets the maximum allowable size for the service.</td>
</tr>
<tr>
<td>Persistent</td>
<td>Bool must be either Yes(default) or No. Keep the content of cache for service over Name Service Restarts. This is useful when paranoia mode is set.</td>
</tr>
<tr>
<td>Maximum-db-size</td>
<td>Number of bytes. Sets the maximum allowable size for the service.</td>
</tr>
</tbody>
</table>
**utils network name-service {hosts|services} cache invalidate**

This command clears the name service cache.

```
utils network name-service {hosts \ services} [cache invalidate]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>Host services cache</td>
</tr>
<tr>
<td>Services</td>
<td>Services service cache</td>
</tr>
</tbody>
</table>

### Command Modes

Administrator (admin:)

### Requirements

- Command privilege level: 1
- Allowed during upgrade: No

Consider the following example for flushing/clearing the cache:

```
admin:utils network name-service hosts cache invalidate
admin:
Successful
```

---

**Addition of Second SAST Role in the CTL File for Recovery**

Earlier releases of Unified Communications Manager that used tokenless approach where endpoints trusted only one Cisco site administrator security token (SAST). This SAST is the CallManager certificate. In this approach, the certificate trust list (CTL) file contained only one SAST record that was used to sign the CTL file. As only one SAST was used, any update in the SAST signer caused the endpoints to get locked out. Following points list the scenarios when endpoints locked out due to update in SAST signer:

- The endpoints accepted the CTL file that is signed by using the CallManager certificate during registration.
- An administrator regenerated the CallManager certificate and updated the CTL file. This regeneration implied that the updated CTL file was signed by updated CallManager certificate instead of the existing CallManager certificate.
- The endpoints did not trust the updated CallManager certificate because the updated certificate was unavailable in the endpoints trust list. So, the endpoints rejected the CTL file instead of downloading it.
- The endpoints tried to connect with the ccm service securely over Transport Layer Security (TLS), ccm service offered its updated CallManager certificate to the endpoints as part of TLS exchange. Because the updated certificate was unavailable in the endpoints trust list, endpoints rejected the CTL file instead of downloading it.
- The phones no longer talk to ccm service and get locked out as a result.

For easier recovery from the end point lock out, the tokenless approach for endpoints is enhanced by addition of second SAST in the CTL File for recovery. In this feature, the tokenless CTL file contains two SAST tokens—the CallManager record and the ITLRecovery record.
The ITLRecovery certificate is chosen over other certificates because of the following reasons:

- Does not change because of secondary reasons, such as change in hostname.
- Already being used in the ITL file.

Certificate Management Changes for ITLRecovery Certificate

In Unified Communications Manager Release 11.0, following changes have been made for the ITLRecovery certificate:

- The validity of ITLRecovery has been extended from 5 years to 20 years to ensure that the ITLRecovery certificate remains same for a longer period.

**Note**

The validity of ITLRecovery certificates continues to be 5 years if you upgrade Unified Communications Manager. While upgrading Unified Communications Manager, the certificates get copied to the later release. However, when you regenerate an ITLRecovery certificate or when you do a fresh install of Unified Communications Manager, the validity of ITLRecovery gets extended to 20 years.

- Before you regenerate an ITLRecovery certificate, a warning message appears on both the CLI and the GUI. This warning message displays that if you use a tokenless CTL and if you regenerate the CallManager certificate, ensure that the CTL file has the updated CallManager certificate and that certificate is updated to endpoints.

View the Validity of ITLRecovery Certificate

**Procedure**

**Step 1**

**Step 2**
Enter search parameters to find a certificate and view its configuration details. The system displays the records that match all the criteria in the Certificate List window.

**Step 3**
Click the ITLRecovery link to view the validity. The validity appears as 20 years from the current year.

**Step 4**
Click OK.

Utils Commands

**utils ctl reset localkey**

This command is used to regenerate the CTL file and sign it with the secondary SAST role (ITLRecovery). Use this command where the CallManager certificate that was used to sign the original CTL file has changed and so, the endpoints are locked out.
utils ctl reset {localkey}

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>localkey</td>
<td>Generates a new CTL file, updates the CTL file on the publisher. The command signs the CTL file with ITLRecovery key.</td>
</tr>
</tbody>
</table>

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

- You must run this command on the Unified Communications Manager publisher node.
- After the endpoints receive the new CTL file, which is signed by ITLRecovery and contains the new CallManager certificate, execute the CTL update command again to sign it with the new CallManager certificate. The CTL file is regenerated but signed by the new CallManager certificate, which is then trusted by the endpoints.

**Requirements**

Command privilege level: 4
Allowed during upgrade: No
Applies to: Unified Communications Manager

---

**Set Command**

**set cert regen ITLRecovery**

This command regenerates the ITLRecovery certificate for the specified unit.

After you type this command, a warning message appears displaying that if you are using a tokenless CTL and if the you are regenerating the CallManager certificate, ensure that the CTL file has the updated CallManager certificate and that certificate is updated to endpoints. To regenerate the certificate, type yes or else type no.

```
set cert regen ITLRecovery
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITLRecovery</td>
<td>Represents the ITLRecovery certificate.</td>
</tr>
</tbody>
</table>

**Command Modes**

Administrator (admin:)

**Requirements**

You must restart the services related to ITLRecovery for the regenerated certificates to become active.

---

**Caution**

You must restart the services related to ITLRecovery for the regenerated certificates to become active.
Command privilege level: 1
Allowed during upgrade: No
Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set cert regen ITLRecovery
```

WARNING: If you are using a tokenless CTL and if the CallManager certificate is recently generated, please ensure that the CTL File already has the new CallManager certificate and is updated to the endpoints, before generating the ITL Recovery certificate. Are you sure want to proceed?

Proceed with regeneration (yes|no)? yes

Successfully Regenerated Certificate for ITLRecovery.

You must restart the services related to ITLRecovery for the regenerated certificates to become active.

### SIP Referred by Header

Starting Release 11.0(1), Cisco Unified Communications Manager will now transparently pass the Referred-By header (present in a incoming REFER message sent by SIP endpoint) to the outbound initial INVITE (triggered by the REFER).

### Session ID Header Support

Starting Release 11.0(1), Cisco Unified Communications Manager will now pass the Session-ID header from inbound to outbound device. Cisco Unified Communications Manager will also generate the device UUID if the associated device does not provide the Session-ID.

### Cisco Endpoints

#### Cisco IP Phones

#### Cisco IP Phone Firmware Versions

The following table lists the latest Cisco IP Phone firmware versions supported for Cisco Unified Communications Manager 11.0.
Table 8: Phone Firmware Versions

<table>
<thead>
<tr>
<th>Phone Family</th>
<th>Firmware Release Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified SIP Phone 3905</td>
<td>9.4(1)SR1</td>
</tr>
<tr>
<td>Cisco Unified IP Phones 6901 and 6911</td>
<td>9.3(1)SR2</td>
</tr>
<tr>
<td>Cisco Unified IP Phones 6921, 6941, 6945, and 6961</td>
<td>6921, 6941, 6961:</td>
</tr>
<tr>
<td></td>
<td>• SIP 9.4(1)</td>
</tr>
<tr>
<td></td>
<td>• SCCP 9.4(1)SR1</td>
</tr>
<tr>
<td></td>
<td>6945: 9.4(1)</td>
</tr>
<tr>
<td>Cisco IP Phone 7800 Series</td>
<td>10.3(1)</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7900 Series</td>
<td>9.4(2)SR1</td>
</tr>
<tr>
<td>Cisco Unified Wireless IP Phone 792x Series</td>
<td>1.4(7)</td>
</tr>
<tr>
<td>Cisco IP Phone 8800 Series</td>
<td>10.3(1)</td>
</tr>
<tr>
<td>Cisco Unified IP Conference Phone 8831</td>
<td>10.3(1)</td>
</tr>
<tr>
<td>Cisco Unified IP Phones 8941 and 8945</td>
<td>9.4(2)SR1</td>
</tr>
<tr>
<td>Cisco Unified IP Phones 8961, 9951, and 9971</td>
<td>9.4(2)SR1</td>
</tr>
</tbody>
</table>

**Cisco Unified SIP Phone 3900 Series Features**

No features have been introduced to the Cisco Unified SIP Phone 3905.

**Cisco Unified IP Phone 6900 Series Features**

No new features were introduced for the Cisco Unified IP Phones 6900 Series.

**Cisco IP Phone 7800 Series Features**


<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Firmware Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Updates</td>
<td>10.3(1)</td>
</tr>
<tr>
<td>User Interface Enhancement</td>
<td>10.3(1)</td>
</tr>
<tr>
<td>Actionable Incoming Call Alert</td>
<td>10.3(1)</td>
</tr>
<tr>
<td>Cisco IP Phone 7811 Support</td>
<td>10.3(1)</td>
</tr>
<tr>
<td>Configurable Energy Efficient Ethernet for Port and Switch</td>
<td>10.3(1)</td>
</tr>
</tbody>
</table>
Cisco Unified IP Phone 7900 Series Features


<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Firmware Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile and Remote Access Through Expressway</td>
<td>10.3(1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Firmware Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable Default Audio Path</td>
<td>9.4(2)SR1</td>
</tr>
</tbody>
</table>

Cisco Unified Wireless IP Phone 792x Series Features


<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Firmware Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager Location</td>
<td>1.4(7)</td>
</tr>
<tr>
<td>Service Support</td>
<td></td>
</tr>
<tr>
<td>PEAP With Server Validation Provisioning</td>
<td>1.4(7)</td>
</tr>
<tr>
<td>Enhancement</td>
<td></td>
</tr>
</tbody>
</table>

Cisco IP Phone 8800 Series Features

The following table lists the features added to the Cisco IP Phone 8800 Series for Firmware Release 10.3(1). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Firmware Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP Phone 8851NR Support</td>
<td>10.3(1)</td>
</tr>
<tr>
<td>Mobile and Remote Access Through Expressway</td>
<td>10.3(1)</td>
</tr>
</tbody>
</table>

Cisco Unified IP Conference Station 8831 Features

No new features were added to the Cisco Unified IP Conference Station 8831.

Cisco Unified IP Phone 8941 and 8945 Features

The following table lists the features added to the Cisco Unified IP Phone 8941 and 8945 for Firmware Release 9.4(2)SR1. For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8900-series/products-release-notes-list.html

Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.0(1)
Cisco Unified IP Phone 8961, 9951, and 9971 Features

No new features were introduced for Cisco Unified IP Phone 8961, 9951, and 9971 Release 9.4(2)SR1.

Cisco DX Series

Cisco DX650, DX70, and DX80 Firmware

The following table lists the latest Cisco DX Series firmware versions supported for Cisco Unified Communications Manager 11.0.

<table>
<thead>
<tr>
<th>Device</th>
<th>Firmware Release Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco DX650</td>
<td>10.2(4)</td>
</tr>
<tr>
<td>Cisco DX70</td>
<td>10.2(4)</td>
</tr>
<tr>
<td>Cisco DX80</td>
<td>10.2(4)</td>
</tr>
</tbody>
</table>

Cisco DX650, DX70, and DX80 Features

The following table lists the features added to the Cisco DX Series for firmware release 10.2(4). For more information, see the Release Notes at the following location:


<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Firmware Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES 256 Encryption</td>
<td>10.2(4)</td>
</tr>
<tr>
<td>AnyConnect VPN version 4.0.01303</td>
<td>10.2(4)</td>
</tr>
<tr>
<td>Mobile and Remote Access through Expressway</td>
<td>10.2(4)</td>
</tr>
</tbody>
</table>
Important Notes

• Features and Services, on page 69
• Interoperability, on page 70
• Miscellaneous, on page 71

Features and Services

6900 Series Phones Fail to Connect When Accessing Personal or Corporate Directories

This information applies to CSCus28530.

6900 series phones may show a connection failed error message when they try to access personal or corporate directories. If you encounter this issue, use the workaround as described here.

Alternatively, you can use the following Cisco Options Package (COP) file: ciscocm.enable_sslv3-v1.0.cop.sgn. To obtain the file from https://software.cisco.com/download/navigator.html, navigate to Downloads > Home > Products > Unified Communications > Call Control > Unified Communications Manager (CallManager) > Unified Communications Manager Version 10.5 > Unified Communications Manager / CallManager / Cisco Unity COnnection Utilities - COP Files.

Caution

The COP file workaround affects your system security.

DTMF Mid-call Features Not Supported for Mobility-enabled Users

For end users who have mobility enabled, DTMF-based mid-call features (for example, *81 - Hold, *83 - Resume) are not supported, regardless of the DTMF Signaling Method setting for the SIP trunk. This issue is present for all SIP trunks due to issues with SIP signaling and MTP allocation. There is no workaround.

For additional details, refer to CSCuu34247, CSCuw95203 and CSCuw95309.

Note

DTMF for User Control Voicemail avoidance and for navigating IVRs at the far-end are both supported.
Jabber Mobile DVOR and EFA Calls to Voicemail Pilot

When a Jabber mobile device places a Dial via Office Reverse (DVOR) or Enterprise Feature Access (EFA) call to a Unity Connection voicemail pilot, the call gets routed to an auto-attendant, rather than directly to their voicemail box. The caller must enter both the mailbox number and PIN to access messages.

This issue exists because when a mobile device sends the Jabber call to Cisco Unified Communications Manager in cellular mode, Cisco Unified Communications Manager does not forward the original calling party number to the voicemail system, regardless of any SIP redirects or diversion header settings for the SIP Trunk. As a result, the caller gets treated as an external caller rather than a user calling their own mailbox to retrieve messages.

Workarounds

Jabber users who want to use DVOR or EFA to call their voicemail can use the following workarounds:

- Use Jabber visual voicemail to retrieve messages
- Use the cellular interface to retrieve messages rather than Jabber

Administrators can configure the following workaround on behalf of Jabber users:

- Configure the voicemail pilot number in the Emergency Number field of the Jabber client. This forces the call to take place over the cellular interface, even if it is called from Jabber.

For additional details, see CSCuw98131.

Media Sense does not record the Consult Call with Selective Recording

When Selective Recording is configured, the Media Sense server does not record the consult call during a transfer. For example, if a call between an agent and a customer is being recorded, and the agent initiates a transfer to another agent, the consult call that takes place between the two agents, prior to the call being transferred, is not recorded.

To ensure that the consult call is recorded, the agent must press the ‘Record’ softkey when the consult call starts.

Interoperability

Interoperability with Cisco TelePresence Management Suite

To interoperate Cisco Unified Communications Manager 11.0(1) with Cisco TelePresence Management Suite, you must run a minimum of Cisco TelePresence Management Suite 14.6.2.

Intercluster Peering Not Supported with Cisco Unified Presence 8.6

Cisco Unified Presence 8.6 is not supported as an intercluster peer for Cisco Unified IM and Presence Service 11.x. For information on supported intercluster peer configurations, see the Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service at http://www.cisco.com/c/en/us/td/docs/
SNMP v3 Restriction with FIPS Mode

When Cisco Unified Communications Manager is operating in FIPS mode, SNMP v3 is not supported with MD5 and DES. To configure SNMP v3 while operating in FIPS mode, you must configure SHA as the authentication protocol and AES 128 as the privacy protocol.

Tomcat Certificate Regeneration with SAML SSO Deployment

If you regenerate Tomcat certificates within a SAML SSO Deployment, you must also generate a new metadata file in Cisco Unified Communications Manager and upload that metadata file to the IdP.

Miscellaneous

Bandwidth Allocations for 88xx SIP Phones

If you are deploying 88xx phones with the SIP protocol, note that these phones will use more bandwidth than the recommended 32 kbps while registering to Cisco Unified Communications Manager. Make sure to take account for the higher bandwidth requirement over registration when you configure your QoS bandwidth allocation in the APIC-EM Controller.

Change Perfmon Counter File Size Parameters in RTMT

If you have started logging perfmon counter data in RTMT and you want to change the file size and maximum number of files, you must first stop counter logging. After you stop the perfmon counters, you can make your changes and then restart perform counters.

Note

The PerfmonCollectCounterData works only for perfmon object that has NO percentage based counters. And for Process and Processor objects the soap API will not work for the CPU %. It's recommended to use the required values for the session based API to get the values which will be perfmonCollectSessionData.

Workaround - First, create a session handle using perfmonOpenSession, and then add the counter using the perfmonAddCounter to use the perfmonCollectSessionData.

Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets

This information applies to CSCtn79567.

Cisco Unified IP Phones 7940 and 7960 do not support Cisco-signed Java Midlets, but they can parse the service information from the phone configuration file.
IM and Presence Service Ad Hoc Group Chat Rooms Privacy Policy

This information resolves CSCuu66150.

An ad hoc group chat room is created when a user starts a group chat session. By default such rooms are open rooms. This means a user who has signed in using a third-party XMPP client such as Psi orPidgin, can discover and join the room and view its chat history. This is only possible through third-party clients because Jabber does not allow room discovery.

Carry out the following steps to work around this problem:

Workaround

1. FromCisco Unified CM IM and Presence Administration, click Messaging > Group Chat and Persistent Chat.

2. In the Member Settings pane, check the following check boxes:
   - Rooms are for members only by default
   - Room owners can change whether or not only moderators can invite people to members-only rooms

3. Uncheck all of the remaining check boxes in the Member Settings pane.

Example

Using this configuration a user who has not been invited to the chat session can discover a room but cannot join it. This solves the problem by making the room a member-only (restricted) room. This configuration also means that participants in the chat session can still invite other users to it so the user experience is not affected.

Other effects of these settings:

- All new ad hoc and persistent rooms are created as members-only.

- If the Cisco XCP Text Conference service is restarted, the existing public rooms become members-only.

- It is not possible for the room moderator or owner to make a new room public.

- Any member of a members-only room can invite another user to be a member of the room. By default, only the room moderator or owner can invite other users.

Note

On Jabber-only deployments, this capability is limited to the room moderator or owner. This is because Jabber does not provide the option for room members to invite other users to a members-only room in its user interface.
MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify

This information applies to CSCu08346.

The calling-line ID (CLID) information is not displayed through Media Gateway Control Protocol (MGCP) IOS gateway after the call is transferred since it does not support Connected Address in ISDN NOTIFY.

Perfect Forward Secrecy is not Supported in IPsec Configuration

This information applies to CSCu74346.

Perfect Forward Secrecy (PFS) security service is not supported in IPsec configuration between Cisco Unified Communications Manager and Voice Gateway.

Route Filter and Associated Route Patterns

When configuring your call routing, make sure that you don't assign a single route filter to too many route patterns. A system core could result if you were to edit a route filter that has hundreds of associated route patterns, due to the extra system processing that is required to update call routing for all of the route patterns that use the route filter. Create duplicate route filters to ensure that this does not occur. For more information see CSCu04938.

TFTP File Size Limit

This information addresses CSCu28887.

You cannot upload files over 250 MB using TFTP file management in the OS Administration interface. If you try, the upload process times out.

To upload files above 250 MB, please work with the Cisco Technical Assistance Center (TAC).

IM and Presence Service Persistent Chat Failover Behavior

This information applies to CSCu40273.

In the event of an IM and Presence Service publisher node failover, the persistent chat rooms created on the database assigned to the failed IM and Presence Service subscriber node are not accessible.

This limitation is being addressed by enhancement request CSCu81931.

IM and Presence Service TSnames File Contains Incorrect Details Following Hostname or IP Address Change

This information applies to CSCu11567.

Use this procedure after you have changed the hostname or IP address on an IM and Presence Service Publisher node, if the tsnames file on the Publisher node contains incorrect details about the updated hostname or IP address.
Procedure

Step 1 On Cisco Unified CM IM and Presence Administration, click Messaging > External Server Setup > External Databases.
Step 2 Click Find to list all the External Databases.
Step 3 Click the External Database connected to the Publisher node and take note of the connection details on the External Database Settings window.
Step 4 Click Delete.
Step 5 To add the database click Add New and enter the details saved from step 3.
Step 6 Click Save.

Persistent Chat Rooms Using Oracle External Database on IM and Presence Service

This information applies to CSCuz84320.

On IM and Presence Service, persistent chat rooms do not work if you are using an Oracle external database and it has not been updated with the patch for the Oracle defect: ORA-22275.

If the patch has not been updated, the following problem occurs in Jabber. When you create a persistent chat room and you do not check the Add Room to My Rooms Tab check box, the room does not appear under the All Rooms tab.

When you restart the Cisco XCP Text Conference Manager service, Jabber gives the following message: Room has been deleted. You then have to recreate the persistent chat room after every Cisco XCP Text Conference Manager service restart.

IM and Presence Server Pings to Jabber Are Not Configurable

IM and Presence server updates the presence status of the user as Unavailable if it does not receive a keep-alive from the client after two 1-minute pings.

The timings for these pings are hard-coded on the server side and are not configurable.
New and Retired Documents

Release 11.0(1) includes changes to the core documentation set for Cisco Unified Communications Manager as the documentation for core system configuration and administration tasks has been consolidated and revised. This section summarizes the retired documents that are no longer published as of this release, and describes the newly created documents that replace them.

Retired Documents

The following documents, which were included in previous releases, have been deprecated and will no longer be published as of this release:

- Cisco Unified Communications Manager Administration Guide (old version)
- Cisco Unified Communications Manager Operating System (OS) Administration Guide
- Cisco Unified Communications Manager System Guide
- Features and Services Guide for Cisco Unified Communications Manager
- Disaster Recovery System Administration Guide for Cisco Unified Communications Manager
- TCP and UDP Port Usage Guide for Cisco Unified Communications Manager

The material from these retired guides has been consolidated and rewritten in a set of new documents that were newly created for this release, and which provide detailed end-to-end tasks for how to configure and maintain Cisco Unified Communications Manager. The following table provides a high-level outline summary of how material from the retired books is presented for 11.0.
Table 9: Deprecated Books and the 11.0 Restructuring

<table>
<thead>
<tr>
<th>Deprecated Book</th>
<th>New 11.0 Guides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager Administration Guide (old version)</td>
<td>Configuration tasks and overview information for the system components now appear in the new System Configuration Guide for Cisco Unified Communications Manager, which provides a detailed end-to-end flow for how to configure the call control system. Field description help can be accessed via the GUI-based online help system.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Operating System (OS) Administration Guide</td>
<td>Administration tasks for the Cisco Unified OS Administration user interface are documented in the new task-based Administration Guide for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager System Guide</td>
<td>The new System Configuration Guide for Cisco Unified Communications Manager provides an end-to-end configuration process flow and overview information for the call control system.</td>
</tr>
<tr>
<td>Features and Services Guide for Cisco Unified Communications Manager</td>
<td>The new Feature Configuration Guide for Cisco Unified Communications Manager provides a detailed configuration and overview information for how to configure features in Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Disaster Recovery System Administration Guide for Cisco Unified Communications Manager</td>
<td>Backup and restore administration tasks now appear in the new task-based Administration Guide for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>TCP and UDP Port Usage Guide for Cisco Unified Communications Manager</td>
<td>The System Configuration Guide for Cisco Unified Communications Manager contains a detailed list of port options that are available in Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>

For detailed information on the new guides that are available for 11.0, see New Documents, on page 76

### New Documents

This section provides details for the new documents that were created as of this release. These new documents provide detailed end-to-end tasks for how to configure and maintain Cisco Unified Communications Manager.

#### System Configuration Guide for Cisco Unified Communications Manager

This new guide provides the task flows and procedures that you need to perform in order to configure the call control system. This guide includes procedures for configuring the following elements of your call control system:

- licensing
- device pools
- system and enterprise parameters
- gateways and trunks
- dial plans
• call admission control
• end users
• endpoint devices
• applications
• media resources
• call handling


Feature Configuration Guide for Cisco Unified Communications Manager

This new guide provides the task flows and procedures that you need to complete in order to configure features on the Cisco Unified Communications Manager system. This guide is meant to complement the new System Configuration Guide for Cisco Unified Communications Manager, and is designed to be used after you configure the call control system.

The Feature Configuration Guide for Cisco Unified Communications Manager provides information about the following:
• features for remote workers
• remote network access
• monitoring and recording
• call center features
• voice messaging
• conferencing
• phone features for placing and receiving calls
• presence and privacy features
• custom features


Administration Guide for Cisco Unified Communications Manager

This new guide provides procedures for operating and maintaining the Cisco Unified Communications Manager system. It includes information about ongoing administrative tasks, such as:
• managing users
• managing devices
• monitoring the system status
• installing security certificates
• managing credential policies and single sign-on
• backing up and restoring the system

CHAPTER 6

Documentation Updates for Defects

- Administration Guide, on page 79
- Bulk Certificate Management, on page 81
- Bulk Administration Guide, on page 82
- CDR Admin Guide, on page 82
- CDR Analysis and Reporting Administration Guide, on page 86
- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, on page 86
- Command Line Interface Reference Guide, on page 87
- Feature Configuration Guide, on page 88
- Installing Cisco Unified Communications Manager, on page 94
- Managed Services Guide, on page 94
- Migration to Cisco Unified Communications Manager Using Prime Collaboration Deployment, on page 94
- Online Help for Cisco Unified Communications Manager, on page 95
- Real-Time Monitoring Tool Guide, on page 100
- Security Guide, on page 100
- Serviceability Guide, on page 104
- System Configuration Guide, on page 107
- System Error Messages, on page 112
- Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, on page 115

Administration Guide

Tomcat Certificate and TFTP Service

This documentation update resolves CSCuv75866.

The following note is omitted from the “Manage Certificates” chapter in Administration Guide for Cisco Unified Communications Manager.
When a Tomcat certificate is regenerated or uploaded, the TFTP service should be deactivated and later activated. Else, the TFTP will continue to offer the old cached self-signed tomcat certificate.

**Insufficient Information About Automatic Fallback**

This documentation update resolves CSCuz01075. The **Deployment models** chapter in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* contains insufficient information about the Automatic Fallback field. The following has been omitted from the guide.

Automatic Fallback IM and Presence Service supports automatic fallback to the primary node after a failover. Automatic fallback is the process of moving users back to the primary node after a failover without manual intervention. You can enable automatic fallback with the Enable Automatic Fallback service parameter on the Cisco Unified CM IM and Presence Administration interface. Automatic fallback occurs in the following scenarios:

- A critical service on Node A fails—A critical service (for example, the Presence Engine) fails on Node A. Automatic failover occurs and all users are moved to Node B. Node A is in a state called “Failed Over with Critical Services Not Running”. When the critical service recovers, the node state changes to "Failed Over." When this occurs Node B tracks the health of Node A for 30 minutes. If no heartbeat is missed in this timeframe and the state of each node remains unchanged, automatic fallback occurs.

- Node A is rebooted—Automatic failover occurs and all users are moved to Node B. When Node A returns to a healthy state and remains in that state for 30 minutes automatic fallback will occur.

- Node A loses communications with Node B—Automatic failover occurs and all users are moved to Node B. When communications are re-established and remain unchanged for 30 minutes automatic fallback will occur.

If failover occurs for a reason other than one of the three scenarios listed here, you must recover the node manually. If you do not want to wait 30 minutes before the automatic fallback, you can perform a manual fallback to the primary node. For example: Using presence redundancy groups, Cisco Jabber clients will fail over to a backup IM and Presence Service node if the services or hardware fail on the local IM and Presence Service node. When the failed node comes online again, the clients automatically reconnect to the local IM and Presence Service node. When the failed node comes online, a manual fallback operation is required unless the automatic fallback option is set. You can manually initiate a node failover, fallback, and recovery of IM and Presence Service nodes in the presence redundancy group. A manual fallback operation is required unless the automatic fallback option is set.

**Certificate Monitor Frequency Interval**

This documentation update resolves CSCvc32210.

The following note is omitted from the “Monitor Certificate Expiration” procedure in the *Administration Guide for Cisco Unified Communications Manager*. 
The certificate monitor service runs every 24 hours by default. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 24 hours. The interval does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the certificate either has expired or is going to expire in one day.

**New System Roles**

This documentation update resolves CSCve54694.

The following table describes the new fields that are omitted from the “Manage User Access” chapter in the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* and “Configure User Access” chapter in the *System Configuration Guide for Cisco Unified Communications Manager*.

<table>
<thead>
<tr>
<th>Standard Role</th>
<th>Privileges/Resources for the Role</th>
<th>Associated Standard Access Control Group(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard SSO Config Admin</td>
<td>Allows you to administrator all aspects of SAML SSO configuration</td>
<td></td>
</tr>
<tr>
<td>Standard Confidential Access Level Users</td>
<td>Allows you to access all the Confidential Access Level Pages</td>
<td>Standard Cisco Call Manager Administration</td>
</tr>
<tr>
<td>Standard CCMADMIN Administration</td>
<td>Allows you to administrator all aspects of CCMAdmin system</td>
<td>Standard Cisco Unified CM IM and Presence Administration</td>
</tr>
<tr>
<td>Standard CCMADMIN Read Only</td>
<td>Allows read access to all CCMAdmin resources</td>
<td>Standard Cisco Unified CM IM and Presence Administration</td>
</tr>
<tr>
<td>Standard CUReporting</td>
<td>Allows application users to generate reports from various sources</td>
<td>Standard Cisco Unified CM IM and Presence Reporting</td>
</tr>
</tbody>
</table>

**Bulk Certificate Management**

This documentation update resolves CSCve78030.

The following note is added in the “Import Certificates” procedure in the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

- Import of certificate using bulk certificate management causes phones to reset.
**Bulk Administration Guide**

**EMCC Device Calculation in the Bulk Administration Tool**

This documentation update resolves CSCuy38765.

The following information is omitted from the “Insert EMCC Devices” procedure in the *Bulk Administration Guide*:

To determine how many EMCC devices to add, look at the number of registered phones and add 5% to account for devices that may not be registered at the moment. If you have 100 phones, multiply 100 by 0.5, which equals 5. You add the result (5) to the total (100). The number of EMCC devices is 105.

To display information about the number of registered phones, gateways, and media resource devices on Cisco Unified Communications Manager, open RTMT and choose **Voice/Video > Device > Device Summary**.

**Incorrect Text Editor for Creating Text-Based CSV File**

This documentation update resolves CSCvd21759.

The “Text-Based CSV Files” chapter in the *Bulk Administration Guide for Cisco Unified Communications Manager* incorrectly state, you can create a CSV data file by using a text editor, such as Microsoft Notepad. The correct text editor to create a CSV data file is Notepad ++.

Using a text editor, such as Notepad++, you can select encoding as UTF-8 without Byte Order Mark (BOM) from the Encoding drop-down.

**CDR Admin Guide**

**Call Termination Cause Codes**

This documentation update resolves CSCut65030.

The “Call Termination Cause Codes” table in the “Call Detail Records” chapter provides details related to call termination cause codes.

The following table contains the correct description for call termination cause code number 19.

**Table 11: Call Termination Cause Codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No error</td>
</tr>
<tr>
<td>1</td>
<td>Unallocated (unassigned) number</td>
</tr>
<tr>
<td>2</td>
<td>No route to specified transit network (national use)</td>
</tr>
<tr>
<td>3</td>
<td>No route to destination</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>4</td>
<td>Send special information tone</td>
</tr>
<tr>
<td>5</td>
<td>Misdialed trunk prefix (national use)</td>
</tr>
<tr>
<td>6</td>
<td>Channel unacceptable</td>
</tr>
<tr>
<td>7</td>
<td>Call awarded and being delivered in an established channel</td>
</tr>
<tr>
<td>8</td>
<td>Preemption</td>
</tr>
<tr>
<td>9</td>
<td>Preemption—circuit reserved for reuse</td>
</tr>
<tr>
<td>16</td>
<td>Normal call clearing</td>
</tr>
<tr>
<td>17</td>
<td>User busy</td>
</tr>
<tr>
<td>18</td>
<td>No user responding</td>
</tr>
<tr>
<td>19</td>
<td>No answer from user (If &quot;No Answer Ring duration&quot; value is greater than the T301 Timer value and after T301 Timer expiry, Call Forwarding No Answer(CFNA) Feature would be invoked).</td>
</tr>
<tr>
<td>20</td>
<td>Subscriber absent</td>
</tr>
<tr>
<td>21</td>
<td>Call rejected</td>
</tr>
<tr>
<td>22</td>
<td>Number changed</td>
</tr>
<tr>
<td>26</td>
<td>Non-selected user clearing</td>
</tr>
<tr>
<td>27</td>
<td>Destination out of order</td>
</tr>
<tr>
<td>28</td>
<td>Invalid number format (address incomplete)</td>
</tr>
<tr>
<td>29</td>
<td>Facility rejected</td>
</tr>
<tr>
<td>30</td>
<td>Response to STATUS ENQUIRY</td>
</tr>
<tr>
<td>31</td>
<td>Normal, unspecified</td>
</tr>
<tr>
<td>34</td>
<td>No circuit/channel available</td>
</tr>
<tr>
<td>38</td>
<td>Network out of order</td>
</tr>
<tr>
<td>39</td>
<td>Permanent frame mode connection out of service</td>
</tr>
<tr>
<td>40</td>
<td>Permanent frame mode connection operational</td>
</tr>
<tr>
<td>41</td>
<td>Temporary failure</td>
</tr>
<tr>
<td>42</td>
<td>Switching equipment congestion</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>43</td>
<td>Access information discarded</td>
</tr>
<tr>
<td>44</td>
<td>Requested circuit/channel not available</td>
</tr>
<tr>
<td>46</td>
<td>Precedence call blocked</td>
</tr>
<tr>
<td>47</td>
<td>Resource unavailable, unspecified</td>
</tr>
<tr>
<td>49</td>
<td>Quality of Service not available</td>
</tr>
<tr>
<td>50</td>
<td>Requested facility not subscribed</td>
</tr>
<tr>
<td>53</td>
<td>Service operation violated</td>
</tr>
<tr>
<td>54</td>
<td>Incoming calls barred</td>
</tr>
<tr>
<td>55</td>
<td>Incoming calls barred within Closed User Group (CUG)</td>
</tr>
<tr>
<td>57</td>
<td>Bearer capability not authorized</td>
</tr>
<tr>
<td>58</td>
<td>Bearer capability not presently available</td>
</tr>
<tr>
<td>62</td>
<td>Inconsistency in designated outgoing access information and subscriber class</td>
</tr>
<tr>
<td>63</td>
<td>Service or option not available, unspecified</td>
</tr>
<tr>
<td>65</td>
<td>Bearer capability not implemented</td>
</tr>
<tr>
<td>66</td>
<td>Channel type not implemented</td>
</tr>
<tr>
<td>69</td>
<td>Requested facility not implemented</td>
</tr>
<tr>
<td>70</td>
<td>Only restricted digital information bearer capability is available (national use)</td>
</tr>
<tr>
<td>79</td>
<td>Service or option not implemented, unspecified</td>
</tr>
<tr>
<td>81</td>
<td>Invalid call reference value</td>
</tr>
<tr>
<td>82</td>
<td>Identified channel does not exist</td>
</tr>
<tr>
<td>83</td>
<td>A suspended call exists, but this call identity does not</td>
</tr>
<tr>
<td>84</td>
<td>Call identity in use</td>
</tr>
<tr>
<td>85</td>
<td>No call suspended</td>
</tr>
<tr>
<td>86</td>
<td>Call having the requested call identity has been cleared</td>
</tr>
<tr>
<td>87</td>
<td>User not member of CUG (Closed User Group)</td>
</tr>
<tr>
<td>88</td>
<td>Incompatible destination</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>90</td>
<td>Destination number missing and DC not subscribed</td>
</tr>
<tr>
<td>91</td>
<td>Invalid transit network selection (national use)</td>
</tr>
<tr>
<td>95</td>
<td>Invalid message, unspecified</td>
</tr>
<tr>
<td>96</td>
<td>Mandatory information element is missing</td>
</tr>
<tr>
<td>97</td>
<td>Message type nonexistent or not implemented</td>
</tr>
<tr>
<td>98</td>
<td>Message is not compatible with the call state, or the message type is nonexistent or not implemented</td>
</tr>
<tr>
<td>99</td>
<td>An information element or parameter does not exist or is not implemented</td>
</tr>
<tr>
<td>100</td>
<td>Invalid information element contents</td>
</tr>
<tr>
<td>101</td>
<td>The message is not compatible with the call state</td>
</tr>
<tr>
<td>102</td>
<td>Call terminated when timer expired; a recovery routine executed to recover from the error</td>
</tr>
<tr>
<td>103</td>
<td>Parameter nonexistent or not implemented - passed on (national use)</td>
</tr>
<tr>
<td>110</td>
<td>Message with unrecognized parameter discarded</td>
</tr>
<tr>
<td>111</td>
<td>Protocol error, unspecified</td>
</tr>
<tr>
<td>122</td>
<td>Precedence Level Exceeded</td>
</tr>
<tr>
<td>123</td>
<td>Device not Preemptable</td>
</tr>
<tr>
<td>125</td>
<td>Out of bandwidth (Cisco specific)</td>
</tr>
<tr>
<td>126</td>
<td>Call split (Cisco specific)</td>
</tr>
<tr>
<td>127</td>
<td>Interworking, unspecified</td>
</tr>
<tr>
<td>129</td>
<td>Precedence out of bandwidth</td>
</tr>
<tr>
<td>131</td>
<td>Call Control Discovery PSTN Failover (Cisco specific)</td>
</tr>
<tr>
<td>132</td>
<td>IME QOS Fallback (Cisco specific)</td>
</tr>
<tr>
<td>133</td>
<td>PSTN Fallback locate Call Error (Cisco specific)</td>
</tr>
<tr>
<td>134</td>
<td>PSTN Fallback wait for DTMF Timeout (Cisco specific)</td>
</tr>
<tr>
<td>135</td>
<td>IME Failed Connection Timed out (Cisco specific)</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>136</td>
<td>IME Failed not enrolled (Cisco specific)</td>
</tr>
<tr>
<td>137</td>
<td>IME Failed socket error (Cisco specific)</td>
</tr>
<tr>
<td>138</td>
<td>IME Failed domain blacklisted (Cisco specific)</td>
</tr>
<tr>
<td>139</td>
<td>IME Failed prefix blacklisted (Cisco specific)</td>
</tr>
<tr>
<td>140</td>
<td>IME Failed expired ticket (Cisco specific)</td>
</tr>
<tr>
<td>141</td>
<td>IME Failed remote no matching route (Cisco specific)</td>
</tr>
<tr>
<td>142</td>
<td>IME Failed remote unregistered (Cisco specific)</td>
</tr>
<tr>
<td>143</td>
<td>IME Failed remote IME disabled (Cisco specific)</td>
</tr>
<tr>
<td>144</td>
<td>IME Failed remote invalid IME trunk URI (Cisco specific)</td>
</tr>
<tr>
<td>145</td>
<td>IME Failed remote URI not E164 (Cisco specific)</td>
</tr>
<tr>
<td>146</td>
<td>IME Failed remote called number not available (Cisco specific)</td>
</tr>
<tr>
<td>147</td>
<td>IME Failed Invalid Ticket (Cisco specific)</td>
</tr>
<tr>
<td>148</td>
<td>IME Failed unknown (Cisco specific)</td>
</tr>
</tbody>
</table>

**CDR Analysis and Reporting Administration Guide**

**Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service**

**Change IP Address or Hostname Using Unified Operating System GUI**

This documentation update resolves CSCvc70649.

The following information is omitted from the “IP Address and Hostname Changes” chapter in the Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service.

Changing the IP address or hostname triggers an automatic self-signed certificate regeneration. This causes all devices in the cluster to reset so that they can download an updated ITL file. If your cluster is using CA-signed certificates, you will need to have them re-signed.
Domain Name Change for Cisco Unified Communications Manager

This documentation update resolves CSCuw76028.

The following information is omitted from the “Domain Name and Node Name Changes” chapter in the Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service Guide.

Update Domain Name for Cisco Unified Communications Manager

You can use the Command Line Interface (CLI) to change the domain name for Cisco Unified Communications Manager. Update the DNS domain name on all applicable nodes using the CLI. The CLI command makes the required domain name change on the node and triggers an automatic reboot for each node.

Before you begin

- Perform all pre-change tasks and the applicable system health checks.
- Ensure to enable the DNS before changing the domain name.
- If the server table has an existing hostname entry, first change the hostname entry of the domain name.

Procedure

Step 1
Log in to Command Line Interface.

Step 2
Enter `run set network domain <new_domain_name>`
The command prompts for a system reboot.

Step 3
Click Yes to reboot the system.
The new domain name gets updated after the system is rebooted

Step 4
Enter the command `show network eth0` to check if the new domain name is updated after the reboot.

Step 5
Repeat this procedure for all cluster nodes.

What to do next

For more information, see the “Post-Change Tasks and Verification” chapter in the Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service guide.

Command Line Interface Reference Guide

`utils dbreplication clusterreset`

This documentation update resolves CSCvf93618.

The `utils dbreplication clusterreset` command is deprecated, instead run `utils dbreplication reset` command to repair replication.

`admin:utils dbreplication clusterreset`
This command is deprecated, please use 'utils dbreplication reset' to repair replication!

Executed command unsuccessfully


**utils ntp server delete**

This documentation update resolves CSCvf91347.

The following information has been omitted from the `Utils Commands` chapter of the Command Line Interface Guide for Cisco Unified Communications Solutions.

It is required to have at least 1 Network Time Protocol (NTP) server configured. Therefore, you cannot delete an NTP server if only one is configured. If you select the option to delete all the NTP servers, the NTP servers are deleted in top down order and the last NTP server on the list does not get deleted.

**Feature Configuration Guide**

**Add Directory Number to a Device**

This documentation update resolves CSCvd22758.

The following note is omitted from the “Add Directory Number to a Device” procedure in the Feature Configuration Guide for Cisco Unified Communications Manager.

---

**Note**

The Calling Search Space (CSS) and partition of DN are mandatory on devices.

The CTI Remote Device should not block its own DN. The CSS is important for the CTIRD device to reach its own DN.

---

**Cisco IPMA Restriction**

This documentation update resolves CSCvc37425.

The following restriction is omitted from the Cisco Unified Communications Manager Assistant Overview chapter in the Feature Configuration Guide for Cisco Unified Communications Manager:

Only one assistant at a time can assist a manager.

**Call Back Phone Support for 7800 and 8800 Series**

The Call Back chapter is missing support information for the Cisco IP Phone 7800 and 8800 Series, which support the Call Back feature. These phones support both a Call Back softkey and a Call Back button.
Call Pickup Restriction

This documentation update resolves CSCuy92491.

The following restriction is omitted from the "Call Pickup" chapter in the Feature Configuration Guide for Cisco Unified Communications Manager:

<table>
<thead>
<tr>
<th>Restriction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Calling Party International Number Prefix - Phone</td>
<td>If you have configured a prefix in the “Incoming Calling Party International Number Prefix - Phone” service parameter, and an international call is placed to a member in the Call Pickup Group, the prefix does not get invoked in the calling party field if the call gets picked up by another member of the Call Pickup Group.</td>
</tr>
</tbody>
</table>

Call Transfer to Hunt Pilot Restriction

This documentation update resolves CSCuw57732.

The following information is omitted from the “Call Transfer” chapter in Feature Configuration Guide for Cisco Unified Communications Manager:

If a call transfer to a hunt pilot is initiated when an announcement is in progress, the call is redirected only after the announcement is complete.

Cisco Unified Communications Manager Sends INVITE Message to VCS

This documentation update resolves CSCuv22205.

The following information is omitted from “Configure a Remote Destination” section in the “Cisco Unified Mobility” chapter:

When an enterprise user initiates a call from a remote destination to Cisco Jabber, Cisco Unified Communications Manager tries to establish a data call with Cisco Jabber by sending an INVITE message to Cisco TelePresence Video Communication Server (VCS). The call is established regardless of receiving a response from VCS.

Client Matter Codes, Forced Authorization Codes, and Failover Calls

This documentation update resolves CSCuv41976.

The following information is omitted from the “Interactions and Restrictions” section of the Client Matter Codes (CMC) and Forced Authorization Codes (FAC) chapter:

CMCs and FACs do not support failover calls.

Conference Now Restriction

This documentation update resolves CSCuv44920.
The following restriction is omitted from the “Conference Now” chapter in the Feature Configuration Guide for Cisco Unified Communications Manager:

No audio announcement will play if the host is the first person to join the conference. However, when the host dials into Conference Now from an internal IP Phone, there is a visual display on the IP Phone showing “To Conference”.

**Note**

If the host joins the Conference Now from any external phone, then there will be no visual display on the phone.

---

**CFUR is not supported by mobile devices**

This documentation update resolves CSCUs09008.

The following restriction is omitted from the “Cisco Unified Mobility” chapter in the Feature Configuration Guide for Cisco Unified Communications Manager:

CFUR settings for mobile devices is not supported. Use Call Forward Busy and Call Forward No Answer rules instead.

**Note**

A busy disconnect cause will be returned if CFUR settings is configured for mobile devices.

---

**Error in EMCC Secure Service URL Configuration**

The “Configure the Extension Mobility Phone Service” procedure in the Configure Extension Mobility Cross Cluster chapter of the Feature Configuration Guide incorrectly states that the secure service URL should be entered in the following format: https://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#

The 8080 port is incorrect. The secure URL requires port 8443. The correct format is: https://<IP Address>:8443/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#.

---

**Client Matter Codes and Force Authorization Codes Not Supported on Cisco Jabber**

This documentation update resolves CSCva32400.

The “Client Matter Codes and Forced Authorization Codes” chapter mentions "Mobile phones with Cisco Jabber installed that support CMCs and FACs" as a prerequisite. This information is inaccurate.

Cisco Jabber does not support CMCs or FACs.

---

**Incorrect Configuration Example for ASA Router**

This documentation update resolves CSCuv20903.
The “Configure ASA for VPN Client on IP Phone” procedure in the “VPN Client” chapter provides an example to configure an IOS router instead of an ASA router.

The following procedure contains the correct example.

**Procedure**

**Step 1**

Complete the local configuration.

a) Configure network interface.

Example:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa# show interface ip brief (shows interfaces summary)
```

b) Configure static routes and default routes.

```
ciscoasa(config)# route <interface_name> <ip_address> <netmask> <gateway_ip>
```

Example:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) Configure the DNS.

Example:

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
```
```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

**Step 2**

Generate and register the necessary certificates for Cisco Unified Communications Manager and ASA.

Import the following certificates from the Cisco Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters).
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

To import these Cisco Unified Communications Manager certificates, do the following:

a) From the Cisco Unified OS Administration, choose Security > Certificate Management.

b) Locate the certificates Cisco_Manufacturing_CA and CAPF. Download the .pem file and save as a .txt file.

c) Create trustpoint on the ASA.
Example:

```plaintext
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following ASA self-signed certificates and register them with Cisco Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

  Example:

  ```plaintext
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Cisco Unified Communications Manager.

  Example:

  ```plaintext
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Register the generated certificate with Cisco Unified Communications Manager.

  Example:

  ```plaintext
ciscoasa(config)# crypto ca export <name> identity-certificate
```

  Copy the text from the terminal and save it as a .pem file and upload it to the Cisco Unified Communications Manager.

**Step 3** Configure the VPN feature. You can use the Sample ASA configuration summary below to guide you with the configuration.
Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyC0ti9 encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
```

**Incorrect Multicast Music On Hold Restriction**

This documentation update resolves CSCvb28136.

In the Music On Hold (MOH) configuration chapter, a restriction incorrectly states that you should configure unicast MOH to avoid silence on the line when an MTP resources is invoked. The correct restriction is as follows:

When an MTP resource gets invoked in a call leg at a site that is using multicast MOH, Cisco Unified Communications Manager falls back to unicast MOH instead of multicast MOH.

**Incorrect Report for Device Mobility**

This documentation update resolves CSCuv20382.

The “Device Mobility” chapter incorrectly states to run a report in Cisco Unified Reporting to determine device support for device mobility. Because this feature is related to Unified Communications Manager and not devices, the report does not apply to device mobility.

In Cisco Unified Reporting, “Mobility” refers to WiFi connections.

**Incorrect URL information for WebDialer**

This documentation update resolves CSCuy13942.

The “WebDialer Overview” topic in the “WebDialer” chapter of the Feature Configuration Guide has incorrect URL to launch Cisco WebDialer from the Directory window.

Following is the correct URL:

```
https://<IP address of Cisco Unified Communications Manager server>:8443/webdialer/ Webdialer
```

**Prerequisite for Private Line Automatic Ringdown Configuration Task Flow for SIP Phones**

This documentation update resolves CSCvd72787.

The following prerequisites are omitted from the “Private Line Automatic Ringdown Configuration Task Flow for SIP Phones” topic in the Feature Configuration Guide for Cisco Unified Communications Manager.

- Create Partition
• Assign Partitions to Calling Search Spaces
• Configure Translation Pattern for Private Line Automatic Ringdown on Phones

Installing Cisco Unified Communications Manager

Install a New Node in an Existing Cluster

This documentation update resolves CSCvd10033.

The following note is omitted from the “Install a New Node in an Existing Cluster” chapter in *Installation Guide for Cisco Unified Communications Manager and IM and Presence Service*.

Note

You can collect the logs from RTMT of a new node added to the existing FQDN cluster, only when you restart the trace collection service. When you sign in to Unified RTMT without restarting the trace collection, the following error message is displayed: *Could not connect to 'Server' <new node name>.*

Managed Services Guide

SNMP Limits

This documentation update resolves CSCuv32781.

The following information is omitted from the “Simple Management Network Protocol” chapter in the *Managed Services Guide*:

Your system does not allow more than ten concurrent polling queries. We recommend a maximum of eight trap destinations; anything higher will affect CPU performance. This requirement applies to all installations regardless of the OVA template that you use.

Migration to Cisco Unified Communications Manager Using Prime Collaboration Deployment

Migrate Cisco Unified Communications Manager to Current Release

This documentation update resolves CSCvg03723.

The following warning is added under the "Migrate Cisco Unified Communications Manager to Current Release" procedure in the *Migration to Cisco Unified Communications Manager Using Prime Collaboration Deployment*. 
It is recommended to migrate the Cisco Unified Communications Manager publisher first, even if you are not using the publisher. This is because there are associated export files created on that publisher and the rest of the process depends on the export files.

For example, if you want to migrate the subscriber, then you have to migrate the Cisco Unified Communications Manager publisher first and then proceed with the migration of subscriber.

---

**Online Help for Cisco Unified Communications Manager**

**Backup Device Limit Incorrect in Disaster Recovery System Online Help**

This documentation update resolves CSCuu94393.

The Disaster Recovery System online help incorrectly states that you can configure up to fourteen backup devices. The correct limit is ten devices.

**Corrected License Report Update Interval**

This documentation update resolves CSCuv84693.

The “License Usage Report” topic in the “Licensing” chapter states that “Usage information is updated once daily”. This statement is incorrect.

The correct update interval for the license report (accessed through System > Licensing > License Usage Report) is once every six hours.

**DHCP Subnet Setup Tips**

This documentation update resolves CSCve07463.

The DHCP subnet setup tip is incorrect in the *Cisco Unified CM Administration Online Help*. The correct information for “DHCP Subnet Setup Tips” is as follows:

Changes to the server configuration do not take effect until you restart DHCP Monitor Service.

**Forbidden String When Configuring Directory Number Alert Names**

This documentation update resolves CSCuv58163.

The following information is omitted from “Directory Number Settings” under topics related to Call Routing.

**Caution**

Do not use the “Alert(” string anywhere in your Alerting Name or ASCII Alerting Name. Use of “Alert(” returns a security protocol error.
Incorrect Time Period Example

This documentation update resolves CSCvb74432.

The time period documentation contains an incorrect example that can cause configuration problems. It suggests to use a date range for a single day time period: "Choose a Year on value of Jan and 1 and an until value of Jan and 1 to specify January 1st as the only day during which this time period applies."

That is incorrect; please avoid using this example for the "Year on...until" option for time periods.

Insufficient Information About Time Schedule

This documentation update resolves CSCvd75418.

The Time Schedule Settings topic in the “Call Routing Menu” chapter of the Cisco Unified CM Administration Online Help contains insufficient information about the selected time period for a day. The following scenario is omitted from the guide:

Table 12: Time Schedule Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Period Information</td>
<td></td>
</tr>
</tbody>
</table>
### Insufficient Information on LDAP User Authentication

This documentation update resolves CSCvc30013.

The *LDAP Authentication Settings* in the *System Menu* chapter in *Cisco Unified CM Administration Online Help* contains insufficient information about LDAP User Authentication. The following note is omitted from the guide:

**Note** You can do LDAP User Authentication using the IP address or the hostname. When IP address is used while configuring the LDAP Authentication, LDAP configuration needs to be made the IP address using the command `utils ldap config ipaddr`. When hostname is used while configuring the LDAP Authentication, DNS needs to be configured to resolve that LDAP hostname.
IP Address Lease Time Default Value

This documentation update resolves CSCuv46131.

The IP address lease time for DHCP server is 43200 seconds (12 hours). In the online help it is documented as seven days (604,800 seconds).

Missing Device Settings Field Descriptions

This documentation update resolves CSCuu83509.

The following setting tables are missing from the “Device Settings” section in the Cisco Unified CM Administration online help:

- Device Defaults Settings
- Default Device Profiles Settings
- Device Profile Settings


Scheduled Date Time Filter Values

This documentation update resolves CSCuv53506.

In the Bulk Administration > Job Scheduler > Find and List Jobs window, to search for jobs use epoch time and not human readable date. For example, search with 1438171 rather than July 2015.

SRTP allowed on ICT does not allow Outbound FastStart

This documentation update resolves CSCuw40390.

The following information was omitted from “H.323 Gateway Configuration Settings” under topics related to Device Menu.

When configuring a non-gatekeeper controlled intercluster trunk on Cisco Unified Communications Manager, if the "SRTP Allowed" setting is checked, the "Outbound FastStart" setting cannot be enabled.

UDS in Remote Cluster Service Configuration is Not Supported

This documentation update resolves CSCuv67224.

In the “Remote Cluster Settings” table under topics related to advanced features, the content about the usage of the UDS check box is incorrect; even though a check box appears on the user interface under Advanced Features > Cluster View, the setting is not supported. User Data Service (UDS) is a service that is enabled by default.
Incorrect Description for Destination Number

This documentation update resolves CSCux74230.

The Remote Destination Configuration Settings field description in the Cisco Unified CM Administration Online Help incorrectly states that you can “Enter the telephone number for the destination”. The correct statement is “Enter the PSTN telephone number for the destination”.

Directory Number Field Description Updated

This documentation update resolves CSCuy28500.

The following note is omitted from the “Directory Number Settings” topic in the online help and “User Device Profile Fields Descriptions in BAT Spreadsheet” topic in the Cisco Unified Communications Manager Bulk Administration Guide:

Note

The “Disable” or “Flash only” setting options apply only for the handset. The led light on the phone button line will still flash.

Insufficient Information About Opus Codec

This documentation update resolves CSCva48193.

The “System Menu” chapter in Cisco Unified CM Administration Online Help contains insufficient information about the Opus Codec field. The following note is omitted from the guide:

Note

The Advertise G.722 Codec service parameter in the Enterprise Parameters Configuration window should be set to Enabled for the SIP devices to use Opus codec. For more information on enterprise parameters, see the System Configuration Guide for Cisco Unified Communications Manager at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/CUCM_BK_SE5DAF88_00_cucm-system-configuration-guide-1151.html.

Remote Destination Configuration Page In the OLH Needs To Be Updated

This documentation update resolves CSCvb88447.

The "Device Menu" chapter in Cisco Unified CM Administration Online Help contains incorrect information in the “Remote Destination Configuration Settings” help page. The following information was either incorrect or omitted in the relevant fields.

• The Timer Information field has incorrect information in the help page. It states the time in “milliseconds”, the correct time is set in “seconds”.

• The Timer Information section lists incorrect order in the help page. The correct orders of the fields are: Delay Before Ringing Timer, Answer Too Soon Timer, and Answer Too Late Timer.

• The Owner User ID field is omitted. Following is the description for this field:
• **Owner User ID**— From drop-down list, choose the appropriate end user profile to which the remote destination profile can be associated later.

## Real-Time Monitoring Tool Guide

### Incorrect Minimum Rate for Monitoring a Performance Counter

This documentation update resolves CSCuz11160.

The *Real-Time Monitoring Tool Guide* states an incorrect minimum amount for monitoring a performance counter. This is the correct statement:

High-frequency polling rate affects the performance on the server. The minimum polling rate for monitoring a performance counter in chart view is 5 seconds; the minimum rate for monitoring a performance counter in table view is 5 seconds. The default for both specifies 10 seconds.

## Security Guide

### CNF File Encryption Is Not Supported by Default on 6901 and 6911, Cisco IP Phones

This documentation update resolves CSCuz68165.

The following note is omitted from the “Phone Models Supporting Encrypted Configuration File” topic in the *Security Guide for Cisco Unified Communications Manager*.

---

**Note**

Cisco Unified IP Phones 6901 and 6911 do not request for the ITL file as they do not support security by default. Therefore, the Cisco Unified Communications Manager cluster should be set to secure (Mixed) mode for the Cisco Unified IP Phones (6901 and 6911) to get the Cisco CTL file containing Cisco Certificate Authority Proxy Function (CAPF) details for the encrypted configuration file to work on the Cisco IP Phones (6901 and 6911).

---

### Certificates

This documentation update resolves CSCvg10775.

The following note is omitted from the “Security Overview” chapter in *Security Guide for Cisco Unified Communications Manager*.

---

**Note**

The maximum supported size of certificate for DER or PEM is 4096 bits.
Enable Password Persistence

This documentation update resolves CSCuy05368.

The following information is omitted from the “Configure VPN Feature Parameters” section of the VPN Feature Setup chapter in the Cisco Unified Communications Manager Security Guide:

When True, a user password gets saved in the phone, if Reset button or “***#***” is used for reset. The password does not get saved and the phone prompts for credentials if the phone loses power or you initiate a factory reset.

Default: False

Incorrect Configuration Example for ASA Router

This documentation update resolves CSCuv20903.

The “Configure ASA for VPN Client on IP Phone” procedure in the “VPN Client” chapter provides an example to configure an IOS router instead of an ASA router.

The following procedure contains the correct example.

Procedure

Step 1  Complete the local configuration.

a) Configure network interface.

Example:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
```

ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto

ciscoasa(config-if)# speed auto

ciscoasa(config-if)# no shutdown
ciscoasa# show interface ip brief (shows interfaces summary)

```

b) Configure static routes and default routes.

ciscoasa(config)# route <interface_name> <ip_address> <netmask> <gateway_ip>

Example:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) Configure the DNS.

Example:

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```
Step 2  Generate and register the necessary certificates for Cisco Unified Communications Manager and ASA.

Import the following certificates from the Cisco Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters).
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

To import these Cisco Unified Communications Manager certificates, do the following:

a) From the Cisco Unified OS Administration, choose Security > Certificate Management.
b) Locate the certificates Cisco_Manufacturing_CA and CAPF. Download the .pem file and save as a .txt file.
c) Create trustpoint on the ASA.
   Example:

```plaintext
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following ASA self-signed certificates and register them with Cisco Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.
  Example:

```plaintext
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Cisco Unified Communications Manager.
  Example:

```plaintext
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```
• Register the generated certificate with Cisco Unified Communications Manager.

Example:

```
ciscoasa(config)# crypto ca export <name> identity-certificate
```

Copy the text from the terminal and save it as a .pem file and upload it to the Cisco Unified Communications Manager.

**Step 3**

Configure the VPN feature. You can use the Sample ASA configuration summary below to guide you with the configuration.

**Note** To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)# service-type remote-access
```

---

**ITL File Size Limitation**

This documentation update resolves CSCvb44649.

The following information is omitted from the “Initial Trust List” chapter of the *Security Guide for Cisco Unified Communications Manager*:

If a Cisco Unified Communications Manager cluster has more than 39 certificates, then the ITL file size on Cisco Unified IP Phone exceeds 64 kilobytes. Increase in the ITL file size affects the ITL to load properly on the phone causing the phone registration to fail with Cisco Unified Communications Manager.

**Resync Bandwidth Option is Removed**

This documentation update resolves CSCuz42447. The *Call Admission Control* chapter in *Cisco Unified Communications Manager System Guide* contains incorrect information about the Bandwidth Calculations field. This option of resync bandwidth is no longer required and the following has been omitted from the guide:

When a link to a location experiences blockage, it may result from bandwidth leakage that has reduced the usable bandwidth for the location. You can resynchronize the bandwidth allotment to the maximum setting for the location without restarting the Cisco Unified Communications Manager server. If you resynchronize the bandwidth for a location when calls are using the link, the bandwidth might be oversubscribed until all calls that are using the link disconnect. An oversubscribed link can cause audio and video quality to degrade. For this reason, resynchronize the location bandwidth during hours when the link has low traffic.

**Support for Certificates from External CAs**

This documentation update resolves CSCve06893.
The following note is omitted from the “Security Overview” chapter in the *Cisco Unified Communications Manager Security Guide*.

---

**Note**  
When using Multi-server (SAN) CA-signed certificates, the Multi-server certificate is only applied to nodes in the cluster at the time the certificate is uploaded to the Publisher. Therefore, anytime a node is rebuilt or a new node is added to the cluster, it is necessary to generate a new Multi-server certificate and upload it to the cluster.

---

### Update ITL File for IP Phones

This documentation update resolves CSCve93055.

The following note is added in the “Update ITL File for IP Phones” section in the *Security Guide for Cisco Unified Communications Manager*.

---

**Note**  
Cisco Unified Communications Manager versions 8.6 and later automatically resets phones after you enable the **Prepare cluster for pre CM-8.0 rollback** Enterprise Parameter. For Central TFTP server's Cisco Unified Communications Manager version and how to enable this parameter, see the "Roll Back Cluster to a Pre-8.0 Release" section in the *Cisco Unified Communications Manager Security Guide*.

---

### Serviceability Guide

#### IM and Presence Security Best Practice

This documentation update resolves CSCuz69271. The following note is omitted from the “Services” chapter in *Cisco Unified Serviceability Administration Guide*.

Devices using IM and Presence are configured to use a Postgres external database to support persistent chat, compliance, and file transfer. However, the connection between IM and Presence server and Postgres is not secured and the data passes without any check. For the services or devices that do not support TLS, there is another way to provide secure communication by configuring IP Sec, which is a standard protocol for secure communications by authenticating and encrypting each IP packet of a communication session.

#### SNMP Limits

This documentation update resolves CSCuv32781.

The following information is omitted from the “Set up SNMP” procedure in the “Simple Management Network Protocol” chapter in the *Serviceability Administration Guide*:

Your system does not allow more than ten concurrent polling queries. We recommend a maximum of eight trap destinations; anything higher will affect CPU performance. This requirement applies to all installations regardless of the OVA template that you use.
Error in SYSLOG-MIB Parameters

This documentation update resolves CSCux59529.

The “CISCO-SYSLOG-MIB Trap Parameters” topic incorrectly lists the command for "Set clogMaxSeverity" as `snmpset -c public -v2c 1<transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>`.

The correct command is `snmpset -c public -v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>`.

Default Alarms in CiscoSyslog File

This documentation update resolves CSCve84930.

The following information is added under "Alarms" chapter in the Cisco Unified Serviceability Administration Guide.

Table 13: Default Alarms in CiscoSyslog File

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLM_IPSecCertUpdated</td>
<td>The IPSec self-signed cert from a peer node in the cluster has been imported due to a change.</td>
</tr>
<tr>
<td>CLM_IPAddressChange</td>
<td>The IP address of a peer node in the cluster has changed.</td>
</tr>
<tr>
<td>CLM_PeerState</td>
<td>The ClusterMgr session state with another node in the cluster has changed to the current state.</td>
</tr>
<tr>
<td>CLM_MsgIntChkError</td>
<td>ClusterMgr has received a message which has failed a message integrity check.</td>
</tr>
<tr>
<td></td>
<td>This can be an indication that another node in the cluster is configured with the wrong security password.</td>
</tr>
<tr>
<td>CLM_UnrecognizedHost</td>
<td>ClusterMgr has received a message from an IP address which is not configured as a node in this cluster.</td>
</tr>
<tr>
<td>CLM_ConnectivityTest</td>
<td>Cluster Manager detected a network error.</td>
</tr>
<tr>
<td>ServiceActivated</td>
<td>This service is now activated.</td>
</tr>
<tr>
<td>ServiceDeactivated</td>
<td>This service is now deactivated.</td>
</tr>
<tr>
<td>ServiceActivationFailed</td>
<td>Failed to activate this service.</td>
</tr>
<tr>
<td>ServiceDeactivationFailed</td>
<td>Failed to deactivate this service.</td>
</tr>
<tr>
<td>ServiceFailed</td>
<td>The Service has terminated abruptly. Service Manager will try to restart it.</td>
</tr>
<tr>
<td>ServiceStartFailed</td>
<td>Failed to start this service. Service Manager will attempt to start the service again.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServiceStopFailed</td>
<td>Unable to stop the specified service after several retries. The service will be marked stopped.</td>
</tr>
<tr>
<td>ServiceRestartFailed</td>
<td>Unable to restart the specified service.</td>
</tr>
<tr>
<td>ServiceExceededMaxStarts</td>
<td>Service failed to start, even after the max restart attempts.</td>
</tr>
<tr>
<td>FailedToReadConfig</td>
<td>Failed to read configuration file. Configuration file might be corrupted.</td>
</tr>
<tr>
<td>MemAllocFailed</td>
<td>Failure to allocate memory.</td>
</tr>
<tr>
<td>SystemResourceError</td>
<td>System call failed.</td>
</tr>
<tr>
<td>ServiceManagerUnexpectedShutdown</td>
<td>Service Manager restarted successfully after an unexpected termination.</td>
</tr>
<tr>
<td>OutOfMemory</td>
<td>The process has requested memory from the operating system, and there was not enough memory available.</td>
</tr>
<tr>
<td>CREATE-DST-RULE-FILE-CLI</td>
<td>New DST rules file is generated from cli. Phones need to be restarted. Not restarting the phones would result in wrong DST start/stop dates.</td>
</tr>
<tr>
<td>CREATE-DST-RULE-FILE-BOOTUP</td>
<td>New DST rules file is generated during bootup. Phones need to be restarted. Not restarting the phones would result in wrong DST start/stop dates.</td>
</tr>
<tr>
<td>CREATE-DST-RULE-FILE-CRON</td>
<td>New DST rules file is generated from cron. Phones need to be restarted. Not restarting the phones would result in wrong DST start/stop dates.</td>
</tr>
<tr>
<td>PermissionDenied</td>
<td>An operation could not be completed because the process did not have authority to perform it.</td>
</tr>
<tr>
<td>ServiceNotInstalled</td>
<td>An executable is trying to start but cannot because it is not configured as a service in the service control manager. The service name is %s.</td>
</tr>
<tr>
<td>ServiceStopped</td>
<td>A service has stopped.</td>
</tr>
<tr>
<td>ServiceStarted</td>
<td>A service has started.</td>
</tr>
<tr>
<td>ServiceStartupFailed</td>
<td>A service has started.</td>
</tr>
<tr>
<td>FileWriteError</td>
<td>Failed to write into the primary file path.</td>
</tr>
</tbody>
</table>
System Configuration Guide

Bandwidth Calculations

This documentation update resolves CSCuz42436. The Call Admission Control chapter in Cisco Unified Communications Manager System Guide contains incorrect information about the Bandwidth Calculations field. It is mentioned that the iLBC call uses 24 kb/s. The correct bandwidth consumption at 20ms should be 31.2kb/s.

Broadcast Algorithm Restrictions with Call Queuing

This documentation update resolves CSCux61414.

The System Configuration Guide for Cisco Unified Communications Manager has incorrectly stated that broadcast algorithm hunt lists are not supported with call queuing.

However, broadcast algorithm hunt lists are supported with call queuing. Cisco recommends that you have no more than 35 directory numbers for a single line group when you use broadcast algorithms with call queuing.

Common Service Ports

This documentation update resolves CSCve02996.

The following information is omitted from the “Cisco Unified Communications Manager TCP and UDP Port Usage” chapter of the System Configuration Guide for Cisco Unified Communications Manager.

Table 14: Common Service Ports

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td>Unified Communications Manager</td>
<td>443, 8443 / TCP</td>
<td>Used for Cisco User Data Services (UDS) requests</td>
</tr>
</tbody>
</table>

Conference Bridges Overview

This documentation update resolves CSCvd37400.

The following note is omitted from the "Configure Conference Bridges" chapter in the System Configuration Guide for Cisco Unified Communications Manager.

Note

When Cisco Unified Communications Manager server is created, the Conference Bridge Software is also created automatically and it cannot be deleted. You cannot add Conference Bridge Software to Cisco Unified Communications Manager Administration.
Correction in Software Conference Bridge Maximum Audio Streams

This documentation update resolves CSCuu4480.

The maximum audio streams per software conference bridge is incorrectly described in the “Conference Bridge Types” section of the System Configuration Guide for Cisco Unified Communications Manager. The following table contains the correct value.

<table>
<thead>
<tr>
<th>Conference Bridge Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Conference Bridge Software</td>
<td>Software conference devices support G.711 codecs by default.</td>
</tr>
<tr>
<td></td>
<td>The maximum number of audio streams for this type equals 256. With 256 streams, a software conference media resource can handle 256 users in a single conference, or the software conference media resource can handle up to 42 conferencing resources with three users per conference.</td>
</tr>
<tr>
<td></td>
<td>Caution If the Cisco IP Voice Media Streaming Application service runs on the same server as the Cisco CallManager service, a software conference should not exceed the maximum limit of 48 participants.</td>
</tr>
</tbody>
</table>

FGT not getting updated for end users

This documentation update resolves CSCux25861.

Conditions

Steps to Reproduce:

Procedure

---

Step 1 Add an AD to the Cisco Unified Communications Manager.
Step 2 Provide a FGT and perform full sync.

The End-users will be synced with the assigned FGT.

The issue is, when we try to modify the FGT and perform a full sync for the associated LDAP, the new FGT modifications will not get updated in the end user page.

Insufficient Information About Adding a New ILS Hub

This documentation update resolves CSCva25662.

The following restriction is omitted from the “Configure Intercluster Lookup Service” chapter of the System Configuration Guide for Cisco Unified Communications Manager.
When adding an additional hub cluster into the ILS network ensure to verify the following conditions are met for the primary ILS hub node:

- Cluster ID is unique across all the hub nodes in the ILS cluster.
- Fully Qualified Domain Name (FQDN) is configured.
- UDS and EM services are running on all of the hub nodes in the ILS cluster.
- DNS primary and reverse resolution are working fine.
- Import consolidated Tomcat certificates from all the hub nodes.

Else, the "version" information will not get displayed in the Find and List Remote Clusters window even after rebooting the clusters or correcting the errors. The workaround is to remove the hub cluster from the ILS network, comply with the above requirements and add the hub cluster back into the ILS network.

### Insufficient Information About Third-Party Restrictions

This documentation update resolves CSCvc16660.

The following restriction is omitted from the “Configure Third-Party SIP Phones” chapter of the System Configuration Guide for Cisco Unified Communications Manager:

<table>
<thead>
<tr>
<th>Restriction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ILS Hub</td>
<td>When adding an additional hub cluster into the ILS network ensure to verify the following conditions are met for the primary ILS hub node:</td>
</tr>
<tr>
<td></td>
<td>• Cluster ID is unique across all the hub nodes in the ILS cluster.</td>
</tr>
<tr>
<td></td>
<td>• Fully Qualified Domain Name (FQDN) is configured.</td>
</tr>
<tr>
<td></td>
<td>• UDS and EM services are running on all of the hub nodes in the ILS cluster.</td>
</tr>
<tr>
<td></td>
<td>• DNS primary and reverse resolution are working fine.</td>
</tr>
<tr>
<td></td>
<td>• Import consolidated Tomcat certificates from all the hub nodes.</td>
</tr>
<tr>
<td></td>
<td>Else, the &quot;version&quot; information will not get displayed in the Find and List Remote Clusters window even after rebooting the clusters or correcting the errors. The workaround is to remove the hub cluster from the ILS network, comply with the above requirements and add the hub cluster back into the ILS network.</td>
</tr>
</tbody>
</table>

### Intercluster Lookup Service Name Correction

This documentation update resolves CSCuy48640.

The “Common Service Ports” table incorrectly describes ILS as Intracluster Lookup Service. The following table contains the correct name.

<table>
<thead>
<tr>
<th>Restriction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ringback tone restriction for Cisco Video Communications Server (VCS) registered to third-party SIP Endpoints</td>
<td>Blind transfer or switch to request the transfer which occurs over VCS registered endpoints with Cisco Unified Communications Manager will not have a ringback tone. If you do a supervised transfer, then you allocate Music On Hold (MOH) but, not a ringback tone.</td>
</tr>
</tbody>
</table>
Locations Media Resource Audio Bit Rate Policy Service Parameter Limitation

This documentation update resolves CSCux90107.

The following information is omitted from the “Enhanced Location Call Admission Control” chapter:

Locations Media Resource Audio Bit Rate Policy service 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. This service parameter does not have any impact if there is no media in one of the call legs. In such cases, location bandwidth manager deducts the maximum hop bandwidth that is configured for the source destination from the available bandwidth of that location.

Logical Partition Policy configuration overlap

This documentation update resolves CSCuw32019.

The following information was omitted from the “Configure a Logical Partitioning Default Policy” procedure in the “Configure Logical Partitioning” chapter in the System Configuration Guide:

If a policy that contained the value Allow is then later changed to Deny, then it remains Deny. The opposite is also true. A policy previously set to Deny, later changed to Allow is an Allow. The Cisco Unified Reporting > Geolocation Policy Report can help you identify policies that overlap.

Phone Support for Multilevel Precedence and Preemption

This documentation update resolves CSCvb37715.

The restrictions in the Multilevel Precedence and Preemption (MLPP) chapter incorrectly state that only SCCP phones support this feature.

SCCP phones and some SIP phones support MLPP. To verify feature support, see the Cisco Unified IP phone administration guide for your model.

Incorrect SSH Password Character Limitation

This documentation update resolves CSCvb33353.

The “Configure Analog Telephone Adaptors” chapter of the System Configuration Guide for Cisco Unified Communications Manager and the “Phone Settings” topic in the “Device Menu” chapter of the Cisco Unified CM Administration Online Help incorrectly state the Secure Shell Password (SSH) alphanumeric or special characters limitation up to 200 characters. The correct character limitation is only up to 127 characters.
Minimum Call Duration for Quality Report Tool to Collect Streaming Statistics

This documentation update resolves CSCve60853.

The following information is omitted from the Configure Diagnostics and Reporting for Cisco Unified IP Phones chapter in the System Configuration Guide for Cisco Unified Communications Manager.

QRT attempts to collect the streaming statistics after a user selects the type of problem by pressing the QRT softkey. A call should be active for a minimum of 5 seconds for QRT to collect the streaming statistics.

Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

This documentation update resolves CSCve53152.

The following information is omitted from the “Cisco Unified Communications Manager TCP and UDP Port Usage” chapter of the System Configuration Guide for Cisco Unified Communications Manager:

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>53/ TCP</td>
<td>Session Initiation Protocol (SIP) phones resolve the Fully Qualified Domain Name (FQDN) using a Domain Name System (DNS)</td>
</tr>
</tbody>
</table>

*Note* By default, some wireless access points block TCP 53 port, which prevents wireless SIP phones from registering when CUCM is configured using FQDN.

SIP Trunks

This documentation update resolves CSCve60892.

The following note is omitted from the “Configure SIP Trunks” chapter in the System Configuration Guide for Cisco Unified Communications Manager.
When Q.SIG is enabled in Small-scale IP telephony (SIPT) from Cluster A to Cluster B, and if “INVITE” is received with anonymous or any text, then the Cisco Unified Communications Manager does not encode it to Q.SIG data. When you decode the same in the leaf cluster, it displays empty and empty number is forwarded.

When Q.SIG is enabled, URI dialing does not respond as expected and if Q.SIG is disabled, then the Cisco Call Back does not respond between two clusters.

### Time of Day routing not Implemented for Message Waiting Indicator

This documentation update resolves CSCva13963.

The following information is omitted from the “Configure Time of Day Routing” topic in the *System Configuration Guide for Cisco Unified Communications Manager*.

Time of Day routing is not implemented for Message Waiting Indicator intercept.

### System Error Messages

#### Missing Device Type ENUM Values

This update is for CSCvg70867.

The *System Error Messages for Cisco Unified Communications Manager* file is missing the following ENUM definitions for the 78XX and 88xx phones.

<table>
<thead>
<tr>
<th>Value</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>508</td>
<td>Cisco IP Phone 7821</td>
</tr>
<tr>
<td>509</td>
<td>Cisco IP Phone 7841</td>
</tr>
<tr>
<td>510</td>
<td>Cisco IP Phone 7861</td>
</tr>
<tr>
<td>544</td>
<td>Cisco IP Phone 8831</td>
</tr>
<tr>
<td>568</td>
<td>Cisco IP Phone 8841</td>
</tr>
<tr>
<td>569</td>
<td>Cisco IP Phone 8851</td>
</tr>
<tr>
<td>570</td>
<td>Cisco IP Phone 8861</td>
</tr>
<tr>
<td>36665</td>
<td>Cisco IP Phone 7811</td>
</tr>
<tr>
<td>36669</td>
<td>Cisco IP Phone 8821</td>
</tr>
<tr>
<td>36670</td>
<td>Cisco IP Phone 8811</td>
</tr>
<tr>
<td>36677</td>
<td>Cisco IP Phone 8845</td>
</tr>
<tr>
<td>36678</td>
<td>Cisco IP Phone 8865</td>
</tr>
</tbody>
</table>
Missing Reason Codes for LastOutOfServiceInformation Alarms

This update is for CSCvd71818.

The System Error Messages for Cisco Unified Communications file is missing some ENUM values for the Reason For Out Of Service parameter within the LastOutOfServiceInformation alarm. Following is a complete list:

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>TCPtimedOut - The TCP connection to the Cisco Unified Communication Manager experienced a timeout error</td>
</tr>
<tr>
<td>12</td>
<td>TCPucmResetConnection - The Cisco Unified Communication Manager reset the TCP connection</td>
</tr>
<tr>
<td>13</td>
<td>TCPucmAbortedConnection - The Cisco Unified Communication Manager aborted the TCP</td>
</tr>
<tr>
<td>14</td>
<td>TCPucmClosedConnection - The Cisco Unified Communication Manager closed the TCP connection</td>
</tr>
<tr>
<td>15</td>
<td>SCCPKeepAliveFailure - The device closed the connection due to a SCCP KeepAlive failure</td>
</tr>
<tr>
<td>16</td>
<td>TCPdeviceLostIPAddress - The connection closed due to the IP address being lost. This may be due to the DHCP Lease expiring or the detection of IP address duplication. Check that the DHCP Server is online and that no duplication has been reported by the DHCP Server</td>
</tr>
<tr>
<td>17</td>
<td>TCPdeviceLostIPAddress - The connection closed due to the IP address being lost. This may be due to the DHCP Lease expiring or the detection of IP address duplication. Check that the DHCP Server is online and that no duplication has been reported by the DHCP Server</td>
</tr>
<tr>
<td>18</td>
<td>TCPclosedConnectHighPriorityUcm - The device closed the TCP connection in order to reconnect to a higher priority Cisco Unified CM</td>
</tr>
<tr>
<td>20</td>
<td>TCPclosedUserInitiatedReset - The device closed the TCP connection due to a user initiated reset</td>
</tr>
<tr>
<td>22</td>
<td>TCPclosedUcmInitiatedReset - The device closed the TCP connection due to a reset command from the Cisco Unified CM</td>
</tr>
<tr>
<td>23</td>
<td>TCPclosedUcmInitiatedRestart - The device closed the TCP connection due to a restart command from the Cisco Unified CM</td>
</tr>
<tr>
<td>Reason Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>24</td>
<td>TCPClosedRegistrationReject - The device closed the TCP connection due to receiving a registration rejection from the Cisco Unified CM</td>
</tr>
<tr>
<td>25</td>
<td>RegistrationSuccessful - The device has initialized and is unaware of any previous connection to the Cisco Unified CM</td>
</tr>
<tr>
<td>26</td>
<td>TCPclosedVlanChange - The device closed the TCP connection due to reconfiguration of IP on a new Voice VLAN</td>
</tr>
<tr>
<td>27</td>
<td>Power Save Plus</td>
</tr>
<tr>
<td>30</td>
<td>Phone Wipe (wipe from CUCM)</td>
</tr>
<tr>
<td>31</td>
<td>Phone Lock (lock from CUCM)</td>
</tr>
<tr>
<td>32</td>
<td>TCPclosedPowerSavePlus - The device closed the TCP connection in order to enter Power Save Plus mode</td>
</tr>
<tr>
<td>100</td>
<td>ConfigVersionMismatch - The device detected a version stamp mismatch during registration Cisco Unified CM</td>
</tr>
<tr>
<td>101</td>
<td>Config Version Stamp Mismatch</td>
</tr>
<tr>
<td>102</td>
<td>Softkeyfile Version Stamp Mismatch</td>
</tr>
<tr>
<td>103</td>
<td>Dial Plan Mismatch</td>
</tr>
<tr>
<td>104</td>
<td>TCPclosedApplyConfig - The device closed the TCP connection to restart triggered internally by the device to apply the configuration changes</td>
</tr>
<tr>
<td>105</td>
<td>TCPclosedDeviceRestart - The device closed the TCP connection due to a restart triggered internally by the device because device failed to download the configuration or dial plan file</td>
</tr>
<tr>
<td>106</td>
<td>TCPsecureConnectionFailed - The device failed to setup a secure TCP connection with Cisco Unified CM</td>
</tr>
<tr>
<td>107</td>
<td>TCPclosedDeviceReset - The device closed the TCP connection to set the inactive partition as active partition, then reset, and come up from the new active partition</td>
</tr>
<tr>
<td>108</td>
<td>VpnConnectionLost - The device could not register to Unified CM because VPN connectivity was lost 109 IP Address Changed</td>
</tr>
<tr>
<td>109</td>
<td>IP Address Changed</td>
</tr>
<tr>
<td>110</td>
<td>Application Requested Stop (service control notify to stop registering)</td>
</tr>
<tr>
<td>111</td>
<td>Application Requested Destroy</td>
</tr>
<tr>
<td>114</td>
<td>Last Time Crash</td>
</tr>
<tr>
<td>200</td>
<td>ClientApplicationClosed - The device was unregistered because the client application was closed</td>
</tr>
<tr>
<td>Reason Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>201</td>
<td>OsInStandbyMode - The device was unregistered because the OS was put in standby mode</td>
</tr>
<tr>
<td>202</td>
<td>OsInHibernateMode - The device was unregistered because the OS was put in hibernate mode</td>
</tr>
<tr>
<td>203</td>
<td>OsInShutdownMode - The device was unregistered because the OS was shut down</td>
</tr>
<tr>
<td>204</td>
<td>ClientApplicationAbort - The device was unregistered because the client application crashed</td>
</tr>
<tr>
<td>205</td>
<td>DeviceUnregNoCleanupTime - The device was unregistered in the previous session because the system did not allow sufficient time for cleanup</td>
</tr>
<tr>
<td>206</td>
<td>DeviceUnregOnSwitchingToDeskphone - The device was unregistered because the client requested to switch from softphone to deskphone control</td>
</tr>
<tr>
<td>207</td>
<td>DeviceUnregOnSwitchingToSoftphone - The device is being registered because the client requested to switch from deskphone control to softphone</td>
</tr>
<tr>
<td>208</td>
<td>DeviceUnregOnNetworkChanged - The device is being unregistered because the client detected a change of network</td>
</tr>
<tr>
<td>209</td>
<td>DeviceUnregExceededRegCount - The device is being unregistered because the device has exceeded the maximum number of concurrent registrations</td>
</tr>
<tr>
<td>210</td>
<td>DeviceUnregExceededLoginCount - The device is being unregistered because the client has exceeded the maximum number of concurrent logons</td>
</tr>
</tbody>
</table>

**Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager**

**Retrieve Chat Rooms on a Replaced Node**

This documentation update resolves CSCuy96037.

The following information is omitted from the “Chat Node Alias Management” topic in the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* guide.

To ensure that the user has access to all the old chat rooms, take a backup of all the existing aliases before deleting a node and assign the same alias to a new node.
Retrieve Chat Rooms on a Replaced Node
Caveats

- Bug Search Tool, on page 117
- Resolved Caveats, on page 118
- Open Caveats, on page 118

Bug Search Tool

The system grades known problems (bugs) according to severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs
- All customer-found bugs

You can search for open and resolved caveats of any severity for any release using the Cisco Bug Search tool, an online tool available for customers to query defects according to their own needs.

To access the Cisco Bug Search tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Follow these steps to use Cisco Bug Search tool:

2. Log in with your Cisco.com user ID and password.
3. If you are looking for information about a specific problem, enter the bug ID number in the Search for: field, and click Go.

Tip

Click Help on the Bug Search page for information about how to search for bugs, create saved searches, and create bug groups.
Resolved Caveats

You can find the latest resolved caveat information for Unified Communications Manager and IM and Presence Service by using the Bug Search tool, an online tool available for customers to query defects according to their own needs.

- You need an account with Cisco.com to use the Bug Search tool to find open and resolved caveats of any severity for any release.

- You can search for Unified Communications Manager and IM and Presence Service by selecting “Model/SW Family” in the Product drop-down list, and entering “Cisco Unified Communications” or “Cisco Unified Communications Manager IM & Presence Service”, and allowing the Bug Search Tool to suggest products.

Open Caveats

Caveats

Open Caveats for Cisco Unified Communications Manager, Release 11.0(1)

The following table lists open caveats that may cause unexpected behavior in the latest Cisco Unified Communications Manager release. Bugs are listed in alphabetical order by component and then in numerical order by severity.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Severity</th>
<th>Component</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuu62403</td>
<td>3</td>
<td>car</td>
<td>CAR PDF report is unable to recognize and display characters other than English</td>
</tr>
<tr>
<td>CSCuu49260</td>
<td>3</td>
<td>cmui</td>
<td>Bulk Admin Tool does not produce correct vendorConfig XML</td>
</tr>
<tr>
<td>CSCuu56786</td>
<td>3</td>
<td>cmui</td>
<td>Add &quot;Mobility User&quot; field in Device Configuration Page of all devices</td>
</tr>
<tr>
<td>CSCuu58824</td>
<td>3</td>
<td>cpi-os</td>
<td>&quot;Accountlocking&quot; Feature Not Migrated Correctly to 10.X</td>
</tr>
<tr>
<td>CSCuu66375</td>
<td>3</td>
<td>cpi-os</td>
<td>Reduce TTL value to one hour so TCP port can get clear</td>
</tr>
<tr>
<td>CSCuu00543</td>
<td>3</td>
<td>cp-mediacontrol</td>
<td>Fax call from H.323 to SIP with MTP fail</td>
</tr>
<tr>
<td>CSCuu64137</td>
<td>3</td>
<td>cp-mediacontrol</td>
<td>Media flow cut in SME dual stack calls where UPDATE is not supported</td>
</tr>
<tr>
<td>Identifier</td>
<td>Severity</td>
<td>Component</td>
<td>Headline</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>-----------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCuu34247</td>
<td>3</td>
<td>cp-mobility</td>
<td>EFA mid call features are failing over SIP ICT w/ No Prefer DTMF</td>
</tr>
<tr>
<td>CSCuu47104</td>
<td>3</td>
<td>cp-sip-trunk</td>
<td>Call manager service crashes due to issues in reaching IM&amp;P server</td>
</tr>
<tr>
<td>CSCuu67940</td>
<td>3</td>
<td>cp-sip-trunk</td>
<td>CUCM sending UPDATE after 183 session progress</td>
</tr>
<tr>
<td>CSCuu69291</td>
<td>3</td>
<td>cp-sip-trunk</td>
<td>CUCM will not handle IPV6 m line for Fax</td>
</tr>
<tr>
<td>CSCuu63627</td>
<td>3</td>
<td>database</td>
<td>URI dialing with &quot;Apostrophe (') fails</td>
</tr>
<tr>
<td>CSCuu58085</td>
<td>3</td>
<td>database-ids</td>
<td>PMR 32360 227 000: Database replication does not complete due to 195.</td>
</tr>
<tr>
<td>CSCuu55380</td>
<td>3</td>
<td>ims</td>
<td>Redundant LDAP hosts are not used</td>
</tr>
<tr>
<td>CSCuu69964</td>
<td>3</td>
<td>ims</td>
<td>IMS FQDN validation fails for case mismatch of FQDN of certificate</td>
</tr>
<tr>
<td>CSCum05343</td>
<td>3</td>
<td>ipma-service</td>
<td>IPMA - Reflective XSS on Login Page</td>
</tr>
<tr>
<td>CSCuu64781</td>
<td>3</td>
<td>media_str_app</td>
<td>CUCM 10.5.2 MTP leaking DTMF digits RFC2833 to OOB for SIP to CTI calls</td>
</tr>
<tr>
<td>CSCuu59477</td>
<td>3</td>
<td>security</td>
<td>SHA1 in CTL file with etoken is wrong if certificate exceeds 3000 bytes</td>
</tr>
<tr>
<td>CSCuu61288</td>
<td>3</td>
<td>selinux</td>
<td>Selinux blocking the logging in of remote account</td>
</tr>
<tr>
<td>CSCuq13927</td>
<td>3</td>
<td>tapiSDK</td>
<td>Addition/Removal of CiscoTSP providers fail intermittently</td>
</tr>
<tr>
<td>CSCut42768</td>
<td>3</td>
<td>tftp</td>
<td>Missed calls are still logged when unchecking &quot;Log Missed Calls&quot; on 79XX</td>
</tr>
<tr>
<td>CSCuu57031</td>
<td>3</td>
<td>webdialer-service</td>
<td>Sensitive info seen in URL</td>
</tr>
</tbody>
</table>

**Open Caveats for IM and Presence Service, Release 11.0(1)**

The following table lists open caveats that may cause unexpected behavior in the latest IM and Presence Service release. These caveats may also be open in previous releases. Bugs are listed in alphabetical order by component and then in numerical order by severity.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Severity</th>
<th>Component</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuu53039</td>
<td>4</td>
<td>config-agent</td>
<td>Ensure all proxy config params that should have defaults, have values</td>
</tr>
<tr>
<td>CSCuu13171</td>
<td>3</td>
<td>config-agent</td>
<td>Moving Offline Messages between servers may cause Config Agent to core</td>
</tr>
<tr>
<td>Identifier</td>
<td>Severity</td>
<td>Component</td>
<td>Headline</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCuu65533</td>
<td>3</td>
<td>database</td>
<td>Presence offline to watchers/self-view when peuritoiuid repl mismatch</td>
</tr>
<tr>
<td>CSCuu65604</td>
<td>3</td>
<td>database</td>
<td>Process node description column regex on IM&amp;P doesn't match one on CUCM</td>
</tr>
<tr>
<td>CSCuo04714</td>
<td>3</td>
<td>epe</td>
<td>HA: IMDB replication overwriting user presence after split brain recover</td>
</tr>
<tr>
<td>CSCus05697</td>
<td>3</td>
<td>epe</td>
<td>DB replication on WAN deployments takes a long time to complete</td>
</tr>
<tr>
<td>CSCut91235</td>
<td>3</td>
<td>epe</td>
<td>PE occasionally remains in a STARTING state after core recovery</td>
</tr>
<tr>
<td>CSCuu41305</td>
<td>3</td>
<td>intercluster</td>
<td>Unnecessary certificate synchronized from an intercluster peer</td>
</tr>
<tr>
<td>CSCuu12885</td>
<td>3</td>
<td>intercluster</td>
<td>User is not getting presence updates of remotely synced group members.</td>
</tr>
<tr>
<td>CSCuu24422</td>
<td>3</td>
<td>security</td>
<td>CUPS repeatedly imports tomcat-trust certificate</td>
</tr>
<tr>
<td>CSCuu57807</td>
<td>3</td>
<td>security</td>
<td>Redundancy for LDAP Enduser authentication does not function</td>
</tr>
<tr>
<td>CSCut75124</td>
<td>3</td>
<td>vos</td>
<td>PlatformConfig.xml corruption on IM&amp;P Publisher after hostname change</td>
</tr>
<tr>
<td>CSCuu51337</td>
<td>3</td>
<td>vos</td>
<td>IM&amp;P Sub upgrade to 11 fails with &quot;No valid upgrade options were found&quot;</td>
</tr>
<tr>
<td>CSCuu31090</td>
<td>3</td>
<td>xcp-aft</td>
<td>AFT process memory grows when Ext FS is full</td>
</tr>
<tr>
<td>CSCut93446</td>
<td>3</td>
<td>xcp-aft</td>
<td>Repeated AFT service restart causing a core</td>
</tr>
<tr>
<td>CSCuu15876</td>
<td>3</td>
<td>xcp-router</td>
<td>XCP Router holds incorrect component status after network loss/recovery</td>
</tr>
<tr>
<td>CSCuu37065</td>
<td>3</td>
<td>xcp-router</td>
<td>Cannot add Empty AD group when over the contact limit</td>
</tr>
<tr>
<td>CSCuo04591</td>
<td>3</td>
<td>xcp-router</td>
<td>MDNS recovery after network down taking too long</td>
</tr>
<tr>
<td>CSCuu58885</td>
<td>3</td>
<td>xcp-router</td>
<td>Presence gets blocked when cache enabled</td>
</tr>
<tr>
<td>CSCuu77026</td>
<td>3</td>
<td>xcp-router</td>
<td>Excess memory growth under heavy performance load</td>
</tr>
</tbody>
</table>