Documentation Update for Defects

- Administration Guide, on page 1
- Bulk Administration Guide, on page 3
- Changing IP Address and Hostname, on page 4
- Command Line Interface Reference Guide, on page 4
- Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, on page 6
- Feature Configuration Guide, on page 6
- Installing Cisco Unified Communications Manager, on page 8
- Online Help for Cisco Unified Communications Manager, on page 8
- Security Guide, on page 11
- System Configuration Guide, on page 12
- System Error Messages, on page 16
- Online Help for IM and Presence Service, on page 20
- Real Time Monitoring Tool Administration Guide, on page 20

Administration Guide

Calling or Called party Transformations Can be Hit with Calling or Called Party Transformation CSS

This documentation update resolves CSCvc90159.

The following information about transformation patterns has been omitted from the *Configure Transformation Patterns* chapter of the *Administration Guide for Cisco Unified Communications Manager*.

It is possible to:

- Hit a Calling Party Transformation Pattern with a Called Party Transformation CSS.
- Hit a Called Party Transformation Pattern with a Calling Party Transformation CSS.

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*.

Note 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.

Missing Information About Managing Phone Firmware

This documentation update resolves CSCvc69988.

The following tasks are missing from the "Manage Device Firmware" chapter in *Administration Guide for Cisco Unified Communications Manager*.

- Set up Default Firmware for a Phone Model
- Set the Firmware Load for a Phone
- Using a Load Server

For more information, see the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-maintenance-guides-list.html.

New System Roles

This documentation update resolves CSCvc54694.

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 1: Standard Roles, Privileges, and Access Control Groups

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SSO Config Admin	Allows you to administer all aspects of SAML SSO configuration	
Standard Confidential Access Level Users	Allows you to access all the Confidential Access Level Pages	Standard Cisco Call Manager Administration
Standard CCMADMIN Administration	Allows you to administer all aspects of CCMAdmin system	Standard Cisco Unified CM IM and Presence Administration
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	Standard Cisco Unified CM IM and Presence Administration

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CUReporting	Allows application users to generate reports from various sources	Standard Cisco Unified CM IM and Presence Reporting

Phone Type Logo in Device Page

This documentation update resolves CSCvf80788.

The following note is update in the "Install a Device Pack or Cisco Options Package File" procedure in the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*:

Note Restart the tomcat services on all nodes, if the phone type logo is not displayed in the Device page post device package installation.

Regenerate Certificate

This documentation update resolves CSCuz82667.

The following information is added in "Regenerate a Certificate" section in *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

If you click the **Regenerate** button in certificate details page, a self-signed certificate with the same key length is regenerated.

To regenerate a self-signed certificate with a new key length of 3072 or 4096, Click **Generate Self-Signed Certificate**.

Bulk Administration Guide

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.

Changing IP Address and Hostname

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.

Command Line Interface Reference Guide

Updates for set password user security and utils network connectivity

This documentation update resolves CSCvf52786.

set password user security

The following note is removed from the "set password user security" topic of the "Set Commands" chapter in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Note Before running the `set user password security` command on the IM and Presence Service servers (nodes), you must first go to the **Cisco Unified CM IM and Presence Administration** > **System** > **CUCM Publisher** window for each IM and Presence Service server (node), and enter the new security password.

utils network connectivity

The following information is omitted from the "utils network connectivity" topic of the "Utils Commands" chapter in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

The `utils network connectivity` command verifies the node network connection to a remote node.

utils network connectivity

This command verifies the node network connection to the first node in the cluster (this connection is only valid on a subsequent node) and to a remote node.

utils network connectivity [{**reset**}] [*hostname/ip address*]

```
utils network connectivity  [hostname/ip address] [port-number] [timeout]
```

Syntax Description

Parameters	Description
connectivity	This command verifies the node network connection to the first node in the cluster. It is also used to check connectivity to a remote node, where there are two mandatory parameters, **hostname/ip address** and **port-number**.
reset	(Optional) Clears previous return codes.
hostname/ip address	• (Optional) Hostname or IP address of cluster node to check network connectivity with the publisher or the first node. • (Mandatory) Hostname or IP address of the host that has to be tested for the TCP connection, to check network connectivity on the remote server.
port-number	(Mandatory) Port number of the host that requires connection test.
timeout	(Optional) Specifies the time in seconds after which port connectivity message is displayed.

Command Modes

Administrator (admin:)

Usage Guidelines

- The **utils network connectivity** [**reset**] *[hostname/ip address]* command is used to check the network connectivity to the publisher or the first node.
- The **utils network connectivity** [**hostname/ip address**] [**port-number**] *[timeout]* command is used to check the network connectivity to a remote server.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

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.

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
```

For more details on **utils dbreplication reset** command, see the "Utils Commands" chapter in the *Command Line Interface Guide for Cisco Unified Communications Solutions* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

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.

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.

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.

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

Extension Mobility Service Error Codes

This documentation update resolves CSCve51354.

The error codes 39, 40,41, and 44 are updated under "Extension Mobility Service Error Codes" section in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Dial Via Office Reverse

This documentation updates resolves CSCvf55794.

The following information is added under “Configure a Mobility Profile” section in "Cisco Unified Mobility" chapter of *Feature Configuration Guide for Cisco Unified Communications Manager*.

Dial Via Office Reverse (DVO-R) Call feature uses enbloc dialing.

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>`.

Online Help for Cisco Unified Communications Manager

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.

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.

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 2: Time Schedule Settings

Field	Description
Time Period Information	

Field	Description
Selected Time Periods	**Scenario:** If multiple time periods are associated to a time schedule and the time periods does not overlap. However, overlap in a day, then the single day period takes precedence and other time periods for that day is ignored. Example 1: Three time periods are defined in the time schedule: Range of Days: Jan 1 - Jan 31: 09:00 - 18:00 Day of Week: Mon - Fri: 00:00 - 08:30 Day of Week: Mon - Fri: 18:30 - 24:00 In this case, even though the times are not overlapping, Range of Days is ignored for a call on Wednesday at 10:00. Example 2: Three time periods are defined in the time schedule: Single Day: Jan 3 2017 (Tues): 09:00 - 18:00 Day of Week: Mon - Fri: 00:00 - 08:30 Day of Week: Mon - Fri: 18:30 - 24:00 In this case, even though the times are not overlapping, Day of Week is ignored for a call on Jan 3 at 20:00. **Note** If Day of Year settings is configured, then the Day of Year settings is considered for the entire day (24 hours) and Day of Week settings, Range of Days settings for that particular day is ignored.

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.

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.

Security Guide

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.

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.

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.

System Configuration Guide

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 3: Common Service Ports

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	Unified Communications Manager	443, 8443 / TCP	Used for Cisco User Data Services (UDS) requests

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.

Feature Group Template Synchronization Issue

This documentation update resolves CSCux25861.

The following information is omitted from the Feature Group Template chapter of the *System Configuration Guide*:

If you modify an existing feature group template and perform a full synchronization for the associated LDAP, the users that are associated with this template are not updated.

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*:

Restriction	Description
ILS Hub	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 the 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*:

Restriction	**Description**
Ringback tone restriction for Cisco Video Communications Server (VCS) registered to third-party SIP Endpoints	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.

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 CSCvc53152.

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*:

From (Sender)	To (Listener)	Destination Port	Purpose
Phone	Unified Communications Manager	53/ TCP	Session Initiation Protocol (SIP) phones resolve the Fully Qualified Domain Name (FQDN) using a Domain Name System (DNS) **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*.

Note 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.

SIP Route Pattern

This documentation update resolves CSCvg31370.

The following information is added in "Global Dial Plan Replication Overview" section of *System Configuration Guide for Cisco Unified Communications Manager*.

Note If the SIP Route Pattern name contains dashes, you must ensure that there are no numerical digits between dashes. However, you can use a combination of letters and numbers or letters only, if there are more than one dash.

Examples of right and wrong SIP Route Patterns are listed in the following:

Right Patterns:

- abc-1d-efg.xyz.com
- 123-abc-456.xyz.com

Wrong Patterns:

- abc-123-def.xyz.com
- 1bc-2-3ef.xyz.com

Block Inbound Call On ILS Network

This documentation resolves CSCvg77238.

The following information is added in the "ILS Interactions" section in *System Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

To block Inbound calls based on calling party number in an ILS-based network, you must include the SIP route pattern's partition in calling party's CSS. For example, if call originates from SIP Trunk then SIP trunk inbound CSS must have SIP route pattern's partition.

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.

Value	Device Type
508	Cisco IP Phone 7821
509	Cisco IP Phone 7841
510	Cisco IP Phone 7861

Value	Device Type
544	Cisco IP Phone 8831
568	Cisco IP Phone 8841
569	Cisco IP Phone 8851
570	Cisco IP Phone 8861
36665	Cisco IP Phone 7811
36669	Cisco IP Phone 8821
36670	Cisco IP Phone 8811
36677	Cisco IP Phone 8845
36678	Cisco IP Phone 8865
36686	Cisco IP Phone 8851NR
36701	Cisco IP Phone 8865NR

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:

Reason Code	Description
10	TCPtimedOut - The TCP connection to the Cisco Unified Communication Manager experienced a timeout error
12	TCPucmResetConnection - The Cisco Unified Communication Manager reset the TCP connection
13	TCPucmAbortedConnection - The Cisco Unified Communication Manager aborted the TCP
14	TCPucmClosedConnection - The Cisco Unified Communication Manager closed the TCP connection
15	SCCPKeepAliveFailure - The device closed the connection due to a SCCP KeepAlive failure
16	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

Reason Code	Description
17	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
18	TCPclosedConnectHighPriorityUcm - The device closed the TCP connection in order to reconnect to a higher priority Cisco Unified CM
20	TCPclosedUserInitiatedReset - The device closed the TCP connection due to a user initiated reset
22	TCPclosedUcmInitiatedReset - The device closed the TCP connection due to a reset command from the Cisco Unified CM
23	TCPclosedUcmInitiatedRestart - The device closed the TCP connection due to a restart command from the Cisco Unified CM
24	TCPClosedRegistrationReject - The device closed the TCP connection due to receiving a registration rejection from the Cisco Unified CM
25	RegistrationSuccessful - The device has initialized and is unaware of any previous connection to the Cisco Unified CM
26	TCPclosedVlanChange - The device closed the TCP connection due to reconfiguration of IP on a new Voice VLAN
27	Power Save Plus
30	Phone Wipe (wipe from CUCM)
31	Phone Lock (lock from CUCM)
32	TCPclosedPowerSavePlus - The device closed the TCP connection in order to enter Power Save Plus mode
100	ConfigVersionMismatch - The device detected a version stamp mismatch during registration Cisco Unified CM
101	Config Version Stamp Mismatch
102	Softkeyfile Version Stamp Mismatch
103	Dial Plan Mismatch
104	TCPclosedApplyConfig - The device closed the TCP connection to restart triggered internally by the device to apply the configuration changes
105	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
106	TCPsecureConnectionFailed - The device failed to setup a secure TCP connection with Cisco Unified CM

Reason Code	Description
107	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
108	VpnConnectionLost - The device could not register to Unified CM because VPN connectivity was lost 109 IP Address Changed
109	IP Address Changed
110	Application Requested Stop (service control notify to stop registering)
111	Application Requested Destroy
114	Last Time Crash
200	ClientApplicationClosed - The device was unregistered because the client application was closed
201	OsInStandbyMode - The device was unregistered because the OS was put in standby mode
202	OsInHibernateMode - The device was unregistered because the OS was put in hibernate mode
203	OsInShutdownMode - The device was unregistered because the OS was shut down
204	ClientApplicationAbort - The device was unregistered because the client application crashed
205	DeviceUnregNoCleanupTime - The device was unregistered in the previous session because the system did not allow sufficient time for cleanup
206	DeviceUnregOnSwitchingToDeskphone - The device was unregistered because the client requested to switch from softphone to deskphone control
207	DeviceUnregOnSwitchingToSoftphone - The device is being registered because the client requested to switch from deskphone control to softphone
208	DeviceUnregOnNetworkChanged - The device is being unregistered because the client detected a change of network
209	DeviceUnregExceededRegCount - The device is being unregistered because the device has exceeded the maximum number of concurrent registrations
210	DeviceUnregExceededLoginCount - The device is being unregistered because the client has exceeded the maximum number of concurrent logons

Online Help for IM and Presence Service

Incorrect Description for Handling Field

This documentation update resolves CSCvc66409.

Third-party profiles have options for **Handling** and **Fire and Forget**, for TC and JSM events. To aviod the confusions in the Compliance Profile Configuration help page, the **Handling** description was updated with correct information.

Existing Statement for JSM and TC Events

Handling

Click **bounce** if errors returned from the compliance server should be bounced back to the originating party or component, click **pass** if they should be discarded. The Handling setting is ignored if Fire and Forget is not chosen.

Updated Statement for JSM and TC Events

Handling

- **Fire and Forget** is unchecked: Click **bounce** if errors returned from the compliance server must be bounced back to the originating party or component. Click **pass** if error must be discarded.
- **Fire and Forget** is checked: Click **bounce** to send packet to compliance server and cancel event back to the originating party or component (cancel event without waiting for response from compliance server). Click **pass** to send packet to compliance server and event will be processed further by the node (do PASS on event without waiting for response from compliance server).

Real Time Monitoring Tool Administration Guide

RTMT TFTP BuildDeviceCount counter never decrease

This documentation update resolves CSCvf34465.

The following note is added in the "Cisco TFTP Server" chapter in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Note For 11.5 and above, you can built the configuration files and serve instead of caching.

When a build happens, BuildDeviceCount increments. When there is request from the phone, counter increases and never decreases. TFTP stable monitoring is not required.