Documentation Updates

Administration Guide

Cisco Unified IP Phone setup Description Character Length

This documentation update resolves CSCut08307.

The character length for the **Description** field is incorrect in the *Cisco Unified Communications Manager Administration Guide*. The following table shows the correct description.

Field	Description
Description	Identify the purpose of the device. You can enter the user name (such as John Smith) or the phone location (such as Lobby) in this field. For Cisco VG248 gateways, begin the description with`VGC<mac address>`. The description can include up to 128 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Correction in IPv6 Address Field

This documentation update resolves CSCun07023.

The description for the **IPv6 Address (for dual IPv4/IPv6)** field in the *Cisco Unified Communications Manager Administration Guide* is incorrect. The following is the correct description.

Field	Description
IPv6 Address (for dualIPv4/IPv6)	This field supports IPv6. If your network uses DNS that can map to IPv6 addresses, you can enter the hostname of the Cisco Unified Communications Manager server. Otherwise, enter the non-link-local IP address of the Cisco Unified Communications Manager server; for information on how to obtain the non-link local IP address, see the *Cisco Unified Communications Manager Features and Services Guide*. This field, which is included in the TFTP configuration file, is used by phones that run SCCP and SIP to retrieve the IPv6 address of the Cisco Unified Communications Manager server. **Tip** Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information. **Tip** In addition to configuring the IPv6 Name field, you must configure the IP Address/Hostname field, so Cisco Unified Communications Manager can support features and devices that use IPv4 (or IPv4 and IPv6).

Correction in Software Conference Bridge Maximum Audio Streams

This documentation update resolves CSCuu44805.

The maximum audio streams per software conference bridge is incorrectly listed as 128 in the "Software Conference Devices" section of the *Cisco Unified Communications Manager Administration Guide*. The correct value is 256.

DHCP Subnet Setup Tips

This documentation update resolves CSCve07463.

The DHCP subnet setup tip is incorrect in the *Cisco Unified Communications Manager Administration Guide*. 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.

Directory Number Field Description Updated

This documentation update resolves CSCur86259.

The following information is omitted from the "Directory Number Settings" topic in the Cisco Unified Communications Manager Administration Guide and online help:

The Directory Number is a mandatory field.

Directory Number Line Behavior in Cisco Unified Communications Manager

This documentation update resolves CSCuo74599.

The following information is omitted in the "Set Up Cisco Unified IP Phone" procedure in the *Cisco Unified Communications Manager Administration Guide*:

After you add a directory number to a phone and click **Save**, the following message appears:

```
Directory Number Configuration has refreshed due to a directory number
change. Please click Save button to save the configuration.
```

Disable Early Media on 180 Correction

This documentation update resolves CSCup68350.

The "SIP Profile Settings" section in the *Administration Guide* contains incorrect information about the **Disable Early Media on 180** check box. The description states that the setting applies to both the 180 and 183 responses, but the setting applies to only the 180 response.

Extension Mobility Now Supports Device Owners

This documentation update resolves CSCun04965.

You can now configure the Owner User ID in the Phone Settings interface if you are using Extension Mobility. Extension Mobility now supports device owners. A note indicating otherwise is listed in error in the *Cisco Unified Communications Manager Administration Guide*.

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.

Hostname and IP Address Field Can Contain a Fully Qualified Domain Name

This documentation update resolves CSCur62680.

The following information is omitted from the **Host Name/IP Address** field description, listed under the "Server Setup" chapter in the *Administration Guide* and the online help.

You can also enter a fully qualified domain name (FQDN) in this field—for example, `cucmname.example.com`.

Note If Jabber clients are used, we recommend that you use an FQDN instead of a hostname so that the Jabber clients can resolve the Unified Communications Manager domain name.

Hostnames in IPv4 and IPv6 Environments

This documentation update resolves CSCun74975.

The following information is omitted from the **IPv6 Address (for dual IPv4/IPv6)** field description under "Server Settings" in the *Cisco Unified Communications Manager Administration Guide*:

You cannot use an IPv4 address as a hostname in a network environment with both IPv4 and IPv6 addresses.

Hub_None Location Correction

This documentation update resolves CSCuu40700.

The "Location" chapter in the *Administration Guide* and online help states that " The Hub_None location specifies unlimited audio bandwidth and unlimited video bandwidth." This information is inacurrate. The correct information for Hub_None is as follows:

Hub_None is an example location that typically serves as a hub linking two or more locations. It is configured by default with unlimited intra-location bandwidth allocations for audio, video, and immersive bandwidth, but you can specify bandwidth allocations for each of these. By default, devices not assigned to other locations are assigned to Hub_None.

ILS Data Sync to be Delayed Until after DB Replication is Completed

This documentation update resolves CSCuh55365.

The following note is omitted from the Directory number settings table in the *Cisco Unified Communications Manager Administration Guide* and from the Learned Global Dial Plan Data section in the *Cisco Unified Communications Manager Features and Services Guide*.

Note Cisco Unified Communications Manager pauses the recording of learned ILS patterns until replication of cluster is successfully established.

ILS Restictions for Directory URIs

This documentation update resolves CSCus74994.

The following information about Directory URIs has been added to the Directory number settings table in the *Cisco Unified Communications Manager Administration Guide*:

The maximum number of directory URIs that the Intracluster Lookup Service (ILS) can replicate is seven.

Incorrect External Call Control Profile Field Description

This documentation update resolves CSCun07467.

The **External Call Control Profile** field is incorrectly described in the *Cisco Unified Communications Manager Administration Guide.* The following table contains the correct description.

Table 1: Directory Number Settings

Field	Description
Directory Number Information	
External Call Control Profile	In Cisco Unified Communications Manager, you enable external call control by assigning an external call control profile to a directory number. If the directory number has an external call control profile assigned to it, and when a call occurs that matches the directory number, Cisco Unified Communications Manager immediately sends a call-routing query to an adjunct route server, and the adjunct route server directs Cisco Unified Communications Manager on how to handle the call. For more information about external call control, see topics related to external call control in the *Cisco Unified Communications Manager Features and Services Guide*. From the drop-down list box, choose the external call profile that you want to assign to the directory number.

Incorrect Information about Deleting Route Patterns

The *Cisco Unified Communications Manager Administration Guide* and online help contain incorrect information about deleting route patterns such as route groups, hunt lists, and hunt pilots.

The following information further explains the context:

The association of any pattern or directory number (DN) to any device is separate from the devices and patterns themselves. As a result, you can delete a route list even if it is currently used for a route pattern. The same applies to hunt lists, hunt pilots, phones, and DNs.

As a best practice, whenever you remove a device, you must ensure that any associated pattern or DN is accounted for in your numbering plan. If you no longer need a pattern or DN, you must delete it separately from the device with which it was associated. Always check the configuration or dependency records before you delete a hunt list.

The following is an example of incorrect information in the guide:

Cisco Unified Communications Manager associates hunt lists with line groups and hunt pilots; however, deletion of line groups and hunt pilots does not occur when the hunt list is deleted. To find out which hunt pilots are using the hunt list, click the Dependency Records link from the Hunt List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

The following is the corrected information:

Cisco Unified Communications Manager associates hunt lists with line groups and hunt pilots. You can delete a hunt list even when it is associated with line groups and hunt pilots. To find out which hunt pilots are using the hunt list, click the Dependency Records link from the Hunt List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

Incorrect Note about User Locales

This documentation update resolves CSCuq42434.

The note about user locales in the Cisco Unified IP Phone settings section of the *Administration Guide* incorrectly states that Cisco Unified Communications Manager uses the user locale that is association with the device pool. The following is the correct note:

Note If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the common device configurations.

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 Call Control Agent Profile Fields

This documentation update resolves CSCuq11351.

The **Call Control Agent Profile** chapter in *Cisco Unified Communications Manager Administration Guide* contains insufficient information about the Call Control Agent Profile configuration fields. The following table contains the detailed information.

The following table describes the Call Control Agent Profile settings.

Table 2: Call Control Agent Profile Settings

Field	Description
Call Control Agent Profile Configuration	
Call Control Agent Profile ID	Enter a unique ID for the Call Control Agent Profile. This ID is associated with the Directory Number. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Primary Softswitch ID	Enter the primary softswitch ID (prefix) of the directory number alias servers. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Secondary Softswitch ID	Enter the secondary softswitch ID (suffix) of the directory number alias servers. The allowed values for this field are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Object Class	Enter the object class name for the directory numbers associated with the call control agent profile. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Subscriber Type	Enter the subscriber type of the directory numbers associated with the call control agent profile. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).
SIP Alias Suffix	Enter the SIP alias suffix. The E.164 number that you specify for the directory number is appended to this suffix when mapping to the SIP Alias field in the LDAP directory. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).

Field	Description
SIP User Name Suffix	Enter the SIP user name suffix. The E.164 number that you specify for the directory number is appended to this suffix when mapping to the SIP User Name field in the LDAP directory. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).

Line Group Deletion Correction

This documentation update resolves CSCuq26110.

The following is a correction to Line Group Deletion.

You can delete a line group that one or more route/hunt lists references. If you try to delete a line group that is in use, Cisco Unified Communications Manager displays an error message.

Tip Dependency Records is not supported for line groups. As a best practice, always check the configuration before you delete a line group.

Location Menu Path

In the *Administration Guide*and online help, the Location field for H.225 and Intercluster Trunk Settings references the **System** > **Locations** menu. The correct menu path is **System** > **Location Info** > **Location**.

Maximum Hunt Timer Restriction

This documentation update resolves CSCuo90637.

The following note is omitted from the *Cisco Unified Communications Manager Administration Guide* and online help for Hunt Group configuration:

Caution Do not specify the same value for the Maximum Hunt Timer and the RNA Reversion Timeout on the associated line group.

Missing Information for Allow Multiple Codecs in Answer SDP

This documentation update resolves CSCup79162.

The following information is omitted from the "SIP Profile Settings" topic in the *Cisco Unified Communications Manager Administration Guide* and online help:

Configure **Allow multiple codecs in answer SDP** for the following:

- Third-party SIP endpoints that support this capability

- SIP trunks to third-party call controls servers that uniformly support this capability for all endpoints

Do not configure this capability for SIP intercluster trunks to Cisco SME or other Cisco Unified Communications Manager systems.

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.

Remove Resource Priority Namespace List Field from SIP Profile Settings

This documentation update resolves CSCun32999.

The **Resource Priority Namespace List** field under **Device** > **Device Settings** > **SIP Profile** is listed in the *Cisco Unified Communications Manager Administration Guide* and online help, but has been removed from the **SIP Profile Configuration** window in Cisco Unified CM Administration.

Self-Provisioning Application Requires Phone Model with Security By Default

This documentation update resolves CSCun13382.

The following note is omitted from the "Self-Provisioning" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Note Phone models (such as Cisco IP Phone 7940 and 7960; IP Communicator series) that do not support the Security By Default (SBD) feature cannot use the Self-Provisioning service. This is because the self-provisioning feature that runs as an Idle URL supports HTTPS certificates only. These phones cannot verify the HTTPS certificates because they do not support the Trust Verification Service (TVS) functionality of the SBD feature.

However, these phones can still use the Self-Provisioning IVR service, provided that the phones themselves support the Self-Provisioning application.

Service Profiles and Device Owner User IDs

This documentation update resolves CSCuu43939.

The following information is omitted from the "Service Profile Setup" chapter in the *Cisco Unified Communications Manager Administration Guide*:

A service profile is applied for a given device only when the owner user ID is specified. In that case, the service profile configured for the respective user is applied.

A note in the Service Profile Settings table is incorrect. The correct note is:

Note If you specify a default service profile, end users that do not have an associated service profile automatically inherit the default service profile settings. In the same manner, any devices that do not have specified a owner user ID inherit the default service profile settings.

SIP Trunk Fields SIP Trunk Status and SIPTrunk Duration

This documentation update resolves CSCun07961.

The following fields are omitted from "SIP Trunk Settings" in the *Cisco Unified Communications Manager Administration Guide*.

Field	Description
SIP Trunk status as determined by SIP OPTIONS Ping	
Full Service status (alarm—SIPTrunkISV) status	All the remote peers that are destinations of the SIP trunk are available. New call requests can be sent to any remote peer through the SIP trunk.
No Service status (alarm—SIPTrunk OOS)	All the remote peers that are destinations of the SIP trunk are unavailable. New call requests cannot be sent out via the SIP trunk.
Partial Service status (alarm—SIPTrunkPartiallyISV)	At least one remote peer is in service, but not all of the remote peers that are destinations of the SIP trunk are available. New call requests can be sent to an available remote peer through the SIP trunk.
Unknown—OPTIONS Ping not enabled	The SIP trunk status is unknown when SIP OPTIONS Ping is not enabled.

Synchronize Trunks and Gatekeeper Sections Are Not Valid

This documentation update resolves CSCuq05944.

The following changes are applicable because the **Apply Config to Selected** button is not available in **Cisco Unified CM Administration** :

- "Synchronize Trunk" section is removed from the "Trunk Setup" chapter
- "Synchronize Gatekeeper" section is removed from the "Gatekeeper Setup" chapter

Transmit UTF8 for Calling Party Name Field Correction

This documentation update resolves CSCup45037.

The *Cisco Unified Communications Manager Administrator Guide* specifies that the SIP trunk field **Transmit UTF-8 for Calling Party Name** uses the user locale setting of the device pool to determine what to send in the Calling Party Name field. However, the device pool does not have a user locale field. It has a network

locale field, and both the Common Device Configuration record, and the Phone record itself have user locale fields.

The following is the process that the SIP trunk uses to obtain the user locale:

If the **Transmit UTF-8 for Calling Party Name** is checked to obtain the locale, the SIP trunk attempts to obtain the locale from the device. If that attempt fails, the SIP trunk attempts to obtain the user locale from the Common Device Configuration, and if that attempt fails, the SIP trunk obtains the user locale that is used for the Enterprise Parameters.

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 FallbackIM 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.

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.

A Server Restart is Required After Uploading a Certificate

This documentation update resolves CSCux67134.

The following is note omitted from the "Upload Certificate or Certificate Chain" chapter in the *Administration Guide* for Cisco Unified Communications Manager:

Note Restart the affected service after uploading the certificate. When the server comes back up you can access the CCMAdmin or CCMUser GUI to verify your newly added certificates in use.

LDAP Authentication Correction

This documentation update resolves CSCux00028.

The "Update LDAP Authentication " section in the *Cisco Unified Communication Manager Administration Guide* contains incorrect information about "LDAP Authentication". The description states that the LDAP synchronization must be disabled to make changes to the LDAP authentication settings. The correct information for "LDAP Authentication" is as follows:

LDAP synchronization must be enabled to make changes to the LDAP authentication settings.

Authenticate with Multiple LDAP Domains

This documentation update resolves CSCuy37309.

Note When you are using the sAMAccountName value for the **LDAP Attribute for User ID** field, you can only authenticate with one LDAP Domain. To authenticate with multiple domains, you need to use the Active Directory Lightweight Directory Service (AD LDS).

Field	Description
LDAP User Search Base	Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup. **Note** This field is mandatory.

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.

Bulk Administration Guide

Bulk Administration Character Length

This documentation update resolves CSCum94975.

The character length for the **User Template Name** field is incorrect in the *Cisco Unified Communications Manager Bulk Administration Guide*. The following table shows the correct description.

Field	Description
User Template Name	Enter a unique name, up to 132 alphanumeric characters, for the user template.

Bulk Administration Gateway Deletion Changes

This documentation update resolves CSCup31813.

The "Delete Cisco Gateway Records Using Query" topic in the *Bulk Administration Guide* contains only a partial list of gateways that you can delete by using query. The following paragraph is the correct information:

You can use a query to locate the gateway records that you want to delete from Cisco Unified Communications Manager. You can only delete CiscoVG200, VG202, VG204, VG224, VG350 and CiscoCatalyst6000 gateways using the Delete Gateway Configuration window.

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 *Cisco Unified Communications Manager Bulk Administration Guide* 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.

Removed Fields in Delete User Device Profiles Custom Configuration

This documentation update resolves CSCup36738.

The following changes are applicable for "Delete User Device Profiles Custom Configuration."

- **Directory Number** field is removed
- Custom is removed from the window title **Delete User Device Profiles Custom Configuration**
- Removed the step: In the Delete drop-down list box choose one of the following options:
  - User
  - Autogenerated
  - All

TAPS and Cisco UCCX with a Standard License

This documentation update resolves CSCus36476.

The following note is omitted from the "Tool for Auto-Registered Phones Support (TAPS)" chapter in the *Bulk Administration Guide*.

Note The TAPS application does not work with a Cisco UCCX Standard license. You must use either an Enhanced or Premium license.

Call Detail Records Administration Guide

Four New Fields in Call Details Record

This documentation update resolves CSCun19226.

The following table describes the new fields that are omitted from the *Call Details Record Administration Guide*.

Field Name	Range of Values	Description
originalCalledPartyPattern	Text String	Numeric string (with special characters) up to 50 characters. This is the pattern to which the original call was placed before any configured translation rules are applied. Default—empty string "".
finalCalledPartyPattern	Text String	Numeric string (with special characters) string up to 50 characters. The pattern of the final called party to which the call is presented until that call is answered or ringing has ended. If no forwarding occurred, this pattern is the same as originalCalledPartyPattern. This field indicates the pattern before any configured translation rules are applied. This value is the same as the finalCalledPartyNumber if the number is a direct match without any translation Default—empty string "".
lastRedirectingPartyPattern	Text String	Numeric string (with special characters) string up to 50 characters. The pattern of the last party which redirected the call to the current called party. If there is no redirection, the field has the same value as the originalCalledPartyPattern. Default—empty string "".

Field Name	Range of Values	Description
huntPilotPattern	Text String	Numeric string (with special characters) string up to 50 characters. The huntPilot pattern as configured in the database. This field is populated only when the HuntPilot member answers the call which is placed either directly or as a result of redirection to the huntPilot. Default - empty string "". If no huntPilot member answers, this field will be empty.

FAC and CMC Code is not Captured in CDR

This documentation update resolves CSCus91749.

The following information about CDR entry for FAC and CMC calls is omitted in the Forced authorization code (FAC) and Client Matter Code (CMC) topic in the Cisco Unified Communications Manager Call Detail Records Administration Guide .

FAC

CDR will now be written for a setup call leg for all the unanswered calls before the call is redirected to another caller if FAC is used to setup the call.

Note This call will not have any connect time since media is not connected for this call. The CDR will be logged regardless of the service parameter **CdrLogCallsWithZeroDurationFlag** if FAC is present in the call.

FAC Example 2

Blind conference using FAC:

1. Call from 136201 to 136111.
2. 136111 answers and speaks for a few seconds.
3. 136201 presses the **Conference** softkey and dials 136203.
4. The user is prompted to enter the FAC code and the user enters 124. FAC code 124 is configured as level 1 and given a name as Forward_FAC.
5. While 136203 is ringing, 136201 presses the **Conference** softkey to complete the conference.
6. 136203 answers the call.
7. The three members in the conference talk for sometime.

8. 136111 hangs up, leaving 136201 and 136203 in the conference. Since there are only two participants in the conference, the conference feature will join these two directly together and they talk for a few seconds.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	60015	60016	60015	60015	60015	60017
origLegCallIdentifier	23704372	23704374	23704373	23704372	23704376	23704377
destLegCallIdentifier	23704373	23704376	23704381	23704380	23704382	23704378
callingPartyNumber	136201	136201	136111	136201	136203	136201
origCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
finalCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
lastRedirectDn	136111	136203	136201	136201	136201	136203
origCause_Value	393216	0	16	393216	393216	0
dest_CauseValue	393216	0	393216	393216	393216	16
authCodeDescription		Forward_FAC				
authorizationLevel	0	1	0	0	0	0
Duration	18	0	37	37	32	38
authorizationCode		124				

Note The setup call CDR for this example is generated even though it is of zero duration since FAC is used for this call.

CMC Example 2

Blind conference using CMC :

1. Call from 136201 to 136111.
2. 136111 answers and speaks for a few seconds.
3. 136201 presses the **Conference** softkey and dials 136203.
4. The user is prompted to enter the CMC code and the user enters 125. CMC code 125 is configured as level 1 and is given a name as Forward_CMC.
5. While 136203 is ringing, 136201 presses the **Conference** softkey to complete the conference.
6. 136203 answers the call.
7. The three members in the conference talk for sometime.

8. 136111 hangs sup, leaving 136201 and 136203 in the conference. Since there are only two participants in the conference, the conference feature will join these two directly together and they talk for a few seconds.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	60025	60026	60025	60025	60025	60027
origLegCallIdentifier	23704522	23704524	23704523	23704522	23704526	23704527
destLegCallIdentifier	23704523	23704526	23704531	23704530	23704532	23704528
callingPartyNumber	136201	136201	136111	136201	136203	136201
origCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
finalCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
lastRedirectDn	136111	136203	136201	136201	136201	136203
origCause_Value	393216	0	16	393216	393216	0
dest_CauseValue	393216	0	393216	393216	393216	16
authCodeDescription		Forward_CMC				
authorizationLevel	0	1	0	0	0	0
Duration	20	0	32	32	25	48
authorizationCode		125				

Note The setup call CDR for this example is generated even though it is of zero duration since CMC is used for this call.

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

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*.

CLI Reference Guide

ILS Troubleshooting Tips Corrections

This documentation update resolves CSCun09203.

The following information applies to the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

utils ils show peer info should be **utils ils showpeerinfo**.

utils ils find route is an invalid command.

Show perf query counter Command Output

This documentation update resolves CSCuo70238.

The following note is omitted from the **show perf query counter** command section in the *Cisco Unified Communications Command Line Interface Guide*.

Note The output that this command returns depends on the number of endpoints that is configured in the Route Groups in Cisco Unified Communications Manager.

Support Removed for utils vmtools status

The `utils vmtools status` CLI command is no longer supported. For VMware status, check the vSphere client instead.

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.

Disaster Recovery System Guide

Supported SFTP Servers

This documentation update resolves CSCur96680.

The following information is omitted from the *Disaster Recovery System Administration Guide*.

Note We recommend that you retest the DRS with your SFTP server after you upgrade your Unified Communications Manager, upgrade your SFTP server, or you switch to a different SFTP server. Perform this step to ensure that these components operate correctly together. As a best practice, perform a backup and restore on a standby or backup server.

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 3: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is provided and tested by Cisco, and supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the *Cisco Prime Collaboration Deployment Admin Guide* before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.
SFTP Server from a Technology Partner	These servers are third party provided, third party tested, and jointly supported by TAC and the Cisco vendor. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade UCM for which versions compatible: https://marketplace.cisco.com
SFTP Server from another Third Party	These servers are third party provided, have limited Cisco testing, and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

Features and Services 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.

Add or Update Hosted DN Pattern Through CSV File

Procedure

Follow one of these procedures, depending on your configuration:

- If the Hosted DN Group is selected by a Call Control Discovery (CCD) Advertising Service:
  a. Create a new Hosted DN Group to perform the upload.
  b. Delete the CCD Advertising Service.
  c. Upload the existing Hosted DN Group.
  d. Recreate the CCD Advertising Service.

  The CCD Advertising Service unpublishes all existing patterns and republishes newly added patterns.
- If the Hosted DN Group is not selected by a CCD Advertising Service, upload a CSV file directly to replace all Hosted DN Patterns.

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*.

Restriction	Description
Incoming Calling Party International Number Prefix - Phone	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.

Call Pickup Group Visual Notification Does Not Support Localization

This documentation bug resolves CSCup04321.

Localization support is not available for call pickup group visual notification, because this notification uses ASCII for the alerting name.

Calling Party Normalization Restriction

This documentation update resolves CSCuo56960.

The following restriction is omitted from the *Features and Services Guide for Cisco Unified Communications Manager*:

When calling or called party transformations are applied at the gateway or route list level, the calling number in the facility information element (IE) for QSIG calls is the post-transformation number. However, the called party in the facility IE is the pre-transformation called party number.

The calling party that is sent after transformation through the gateway is typically localized and does not cause an issue with the display and routing. The called party is typically the dialed digits and is displayed on the calling phone, so the transformation is not relayed for called party transformations. Called party transformation is designed to send the information based on the gateway that the call is going through, regardless of how the number is dialed. Called party transformation is kept at the gateway level and not updated, whereas the calling party is updated.

CiscoIPMA 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.

Cisco Unified Communications Manager Sends INVITE Message to VCS

This documentation update resolves CSCuv22205.

The following information is omitted from 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 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.

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.

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.

Corrections for the Immediate Divert Feature

This documentation update resolves CSCun20448.

Steps 6 and 7 are incorrect for the “Configure Immediate Divert” procedure in the *Features and Services Guide*. The following are the corrected steps.

Configure Immediate Divert

Step 6

Standard User or Standard Feature softkey is copied to a new template and then the template is used to assign iDivert softkey. Assign the softkey in the Connected, On Hold, and Ring In states. Divert softkey in Cisco Unified IP Phones 8900 series gets enabled using the softkey template and for the 9900 series the Divsert softkey feature gets enabled using feature control policy template.

Step 7

In the Phone Configuration window, assign the newly configured softkey template which has iDivert enabled, to each device that has immediate divert access.

System requirements for Immediate Divert

The following table lists the phones that use the Divert or iDivert softkey. The 8900 and 9900 series contain system requirement changes:

- Cisco Unified Communications Manager 6.0 or later
- ***Table 4: Cisco Unified IP Phones That Use iDivert or Divert Softkeys***

Cisco Unified IP Phone Model	Divert Softkey	iDivert Softkey	What to configure in softkey template
Cisco Unified IP Phone 6900 Series (except 6901 and 6911)	X		iDivert
Cisco Unified IP Phone 7900 Series		X	iDivert
Cisco Unified IP Phone 8900 Series	X		iDivert
Cisco Unified IP Phone 9900 Series	X		iDivert

Cisco Unified Mobility Documentation Changes

This documentation update resolves CSCun14245.

Replace references to *Cisco Unified Mobile Communicator* with *dual-mode phones*.

For example, "a Cisco Unified Mobile Communicator-enabled dual-mode mobile identity" should read "a dual-mode phone mobile identity."

The following parameters are omitted from the Remote Destination Configuration fields:

- **Owner User ID**—From the drop-down list, choose the user ID of the assigned Remote Destination user. The user ID is recorded in the call detail record (CDR) for all calls made from this device.
- **Enable Unified Mobility Features**—Check this check box to enable Unified Mobility features for this remote destination.
- **Enable Extend and Connect**—Check this check box to allow this phone to be controlled by CTI applications (for example, Jabber). For more information, see the *Features and Services Guide for Cisco Unified Communications Manager*.

Replace the parameter field **Mobile Phone** with **Enable Move to Mobile**. Replace the parameter field **Enable Cisco Unified Mobility** with **Enable Single Number Reach**.

Default Partitions

This documentation update resolves CSCum99459.

The following partitions are Cisco-provided default partitions:

- Directory URI
- Global Learned E.164 Numbers
- Global Learned E.164 Patterns
- Global Learned Enterprise Numbers
- Global Learned Enterprise Patterns

For information about Global Learned E.164 Numbers, Global Learned E.164 Patterns, Global Learned Enterprise Numbers, and Global Learned Enterprise Patterns, see the "Partitions for Learned Patterns Settings" section in the *Features and Services Guide for Cisco Unified Communications Manager*.

Directory URI

The Directory URI is a system partition, introduced in Cisco Unified Communications Manager Release 9.0(1), which Cisco Unified Communications Manager automatically creates based on the Directory URIs that are provisioned in the **End User Configuration** window and an association between end users and DNs through a primary extension. You can edit the Directory URI partition but cannot delete it.

For more information about Directory URIs, see the "URI Dialing" chapter in the *Features and Services Guide for Cisco Unified Communications 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.

Force Authorization Codes Not Supported on Cisco Jabber

This documentation update resolves CSCuz63406.

The “Client Matter Codes and Forced Authorization Codes” chapter states that "Mobile phones with Cisco Jabber installed support CMC and FAC." This information is inaccurate. The correct information is as follows:

Mobile phones with Cisco Jabber installed support only CMC. FACs are not supported.

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.

Jabber Devices Count as Registered Devices

This documentation update resolves CSCur73944.

The following information is omitted from the Limitations section of the “Cisco Unified Mobility” chapter in the *Features and Services Guide*.

When initially configured, Jabber devices count as registered devices. These devices increase the count of registered devices in a node, set by the **Maximum Number of Registered Devices** service parameter.

Locations Media Resource Audio Bit Rate Policy Service Parameter Limitation

This documentation update resolves CSCux90107.

The following information is omitted from the “Location Bandwidth Service Parameters” section in the “Enhanced Location Call Admission Control” chapter:

The Locations Media Resource Audio Bit Rate Policy 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.

Music On Hold and Native Call Queuing Behavior

The *Announcements with Music On Hold* document discusses Native Call Queuing and the added capabilities that are related to customized audio announcements and Music On Hold. Access this document at the following URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-technical-reference-list.html

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

Remote Destination and Auto Answer

This documentation update resolves CSCtd43582.

The following restriction is omitted from the "Cisco Mobility" chapter in the *Features and Services Guide for Cisco Unified Communicatins Manager*:

A remote destination call does not work when Auto Answer is enabled.

Restart Intercluster Lookup Service

This documentation update resolves CSCuv11445.

The following information is omitted from "ILS Troubleshooting Tips" in the "Intercluster Lookup Service" chapter of the *Features and Services Guide*:

If you receive an error message when trying to establish ILS between your clusters, you can try to restart the Cisco Intercluster Lookup service from Cisco Unified Serviceability Administration.

SAF Forwarder and Requesting Service Arrow Keys Removed

This documentation update resolves CSCun02017.

The "SAF Forwarder Configuration" and "CCD Requesting Service Configuration" topics in the *Features and Services Guide for Cisco Unified Communications Manager* state that you can order items in a pane by highlighting them and clicking the up and down arrows to the right of the pane. This function was removed from the administrative interface.

SAML Not Enabled after Upgrade on Web Dialer

This documentation update resolves CSCun17524.

The following procedure is omitted from "Enable SAML SSO" section in the *Cisco Unified Communications Manager Features and Services Guide*.

Follow this procedure to enable SAML Single Sign-On (SSO) on Cisco Web Dialer after an upgrade.

Procedure

Step 1 Deactivate the Cisco Web Dialer web service if it is already activated.

Step 2 Disable SAML SSO if it is already enabled.

Step 3 Activate the Cisco Web Dialer web service.

Step 4 Enable SAML SSO.

SAML SSO Authentication LDAP Attribute for User ID Setting

This documentation update resolves CSCuq44567.

The following note is missing from the "SAML Single Sign-On" chapter in *Feature and Services Guide for Cisco Unified Communications Manager*.

Note Cisco Unified Communications Manager currently supports only sAMAccountName option as the LDAP attribute for user ID settings.

Video Capabilities and Enhanced Location Call Admission Control

This documentation update resolves CSCut20187.

The following information is omitted from the Limitations section in the "Enhanced Location Call Admission Control" chapter:

If video capabilities are enabled, then bandwidth for audio will be allocated from video.

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>`.

JTAPI Developers Guide

MeetMe: Unsupported JTAPI Feature

This documentation update resolves CSCum39340.

Applications that use JTAPI, including Unified Contact Center Express (UCCX), are unable to dial MeetMe conference numbers to begin a MeetMe conference or join an already started MeetMe conference. MeetMe is not a feature supported by JTAPI and therefor any application that uses JTAPI for call control is unable to perform actions on MeetMe conferences. For Unified Contact Center Express (UCCX), this prevents MeetMe conferences DN from being the destination of Place Call script steps.

Unsupported CTI Events From SIP Phones

This information resolves CSCur36240.

The *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager* and the *Cisco Unified TAPI Developers Guides for Cisco Unified Communications Manager* do not provide details on the following CTI events. These CTI events are not supported for SIP phones. Developers who are programming third party applications that invoke these CTI events should use SCCP phones.

- CallOpenLogicalChannelEvent
- CallRingEvent
- DeviceLampModeChangedEvent
- DeviceModeChangedEvent
- DeviceDisplayChangedEvent
- DeviceFeatureButtonPressedEvent
- DeviceKeyPressedEvent
- DeviceLampModeChangedEvent
- DeviceRingModeChangedEvent

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.

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.

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".

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 5: 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.

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.

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.

OS Administration Guide

Documentation Update for Certificate Monitor Configuration

This documentation update resolves CSCuo30610.

The following information is omitted from the Certificate Monitor Field Descriptions table:

You can enter multiple email addresses by separating the email addresses with a semicolon (;). Do not insert a space between the email addresses. For example, **`test@cisco.com;test1@cisco.com;test2@cisco.com`**, and so on.

Add CA Signed CAPF Root Certificate to Trust Store

This documentation update resolves CSCut87382.

The following procedure is omitted from the “Manage Certificates” section in the “Security” chapter.:

When using a CA signed CAPF Certificate, follow these steps to add the root certificate to the CallManager trust store.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain**.

Step 3 In the **Upload Certificate/Certificate chain** popup window, select **CallManager-trust** from the **Certificate Purpose** drop-down list and browse to the CA signed CAPF root certificate.

Step 4 After the certificate appears in the **Upload File** field, click **Upload**.

Real-Time Monitoring Tool Guide

Analyze Call Path Tool does not Work with Non-English Language

This documentation update resolves CSCuq28511.

The following note is omitted from the "Cisco Unified Analysis Management" chapter in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Caution The Analyze Call Path Tool might not work correctly if your computer is set to a language other than English.

Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert

This documentation update resolves CSCuq39087.

The default threshold value for LogPartitionLowWaterMarkExceeded alert is incorrectly described in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. The following table contains the correct value.

Table 6: Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds Low Water Mark (90%)

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.

LowAvailableVirtualMemory Threshold Value is Incorrect

This documentation update resolves CSCuu72197.

The LowAvailableVirtualMemory threshold value in the *Cisco Unified Real-Time Monitoring Tool Administration Guide* is incorrectly listed as below 30%. The correct value is below 25%.

FQDN Support to Display Hostnames in RTMT

This documentation update resolves CSCun02558.

To use the Trace and Log Central feature, make sure that the Cisco Unified Real-Time Monitoring Tool can directly access the node or all of the nodes in a cluster without Network Address Translation (NAT). If you configured a NAT to access devices, configure the nodes with a hostname instead of an IP address and make sure that the hostnames (Fully Qualified Domain Name of the host) and their routable IP address are in the DNS node or host file.

RTMT Mail Server Procedure Correction

This documentation update resolves CSCun08876.

The "Add or Edit Mail Server" procedure contains an incorrect step: "In the **Sender UserID** field, enter the sender user ID that you need to notify." The Cisco Unified Real-Time Monitoring Tool does not have a Sender UserID field; disregard this step.

Security Guide

Bulk Certificate Import May Cause Phones To Restart

This documentation update resolves CSCun32117.

The following note is omitted from the Bulk certificate export section in the *Cisco Unified Communications Manager Security Guide* and the Configure EMCC section in the *Cisco Unified Communications Manager Features and Services Guide*.

Note When you use the Bulk Certificate Management tool to import certificates, it will cause an automatic restart of the phones on the cluster on which you imported the certificate.

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.

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).

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 asa `.txt` file.
c) Create trustpoint on the ASA.

Example:

```
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:

```
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:

```
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.

Replace ASA Certificate on AnyConnect VPN Phone

Note When you upload an updated certificate with the same Common Name (CN) to Phone-VPN-trust, you overwrite the old certificate. Upload the new certificate to the subscriber instead of the publisher. Phone-VPN-trust does not replicate to other servers but this process will still add the new certificate to the database for the Phone VPN Gateway configuration. Therefore, the old certificate will not be overwritten.

Procedure

Step 1 Install the new ASA certificate on the ASA, but do not activate it.

Step 2 Add the new ASA certificate to the trust store (Phone-VPN-trust).

Step 3 Add the new ASA certificate to VPN Gateway Configuration. Select and add the new ASA certificate to “VPN certificates in this location.”

Step 4 Gather information about which VPN phones are registering and which VPN phones are not registering.

Step 5 Apply the new configuration file to the phones from the **Common Phone Profile Configuration** window that is used for VPN phones or from the **Device Pool Configuration** window that used for VPN phones.

Step 6 Reset the VPN phones.

Step 7 Ensure that the phone received the updated configuration file or verify that the phone has the new ASA certificate hash information in its configuration file.

For more information, see https://supportforums.cisco.com/document/33891/ip-phone-ssl-vpn-asa-using-anyconnect.

Step 8 Activate the new ASA certificate on the ASA.

Step 9 Verify that the previously registered VPN phones are registering back to Unified Communications Manager.

Step 10 Repeat Steps 4, 5, 6, and 8.

Step 11 Remove the old ASA certificate from the VPN Gateway Configuration.

Secure and Nonsecure Indication Tone

This documentation update resolves CSCuq04604.

In the *Cisco Unified Communications Manager Security Guide*, the section about secure and nonsecure indication tones states that "Protected devices can call nonprotected devices that are either encrypted or nonencrypted. In such cases, the call specifies nonprotected and the nonsecure indication tone plays." This statement applies only if a protected phone calls a nonencrypted, nonprotected phone. If the call is encrypted for both parties, the indication tone plays the secure tone.

Protected devices that call nonprotected devices that are encrypted play the secure tone, while protected devices that call nonprotected and nonencrypted devices play the nonsecure tone.

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.

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.

Serviceability Guide

Cisco CAR DB Service

This documentation update resolves CSCup98304.

The following service is omitted from the “Services” chapter in the *Cisco Unified Communications Manager Serviceability Guide* and online help.

Cisco CAR DB Service

Cisco CAR DB manages the Informix instance for the CAR database, which allows Service Manager to start or stop this service and to bring up or shut down the CAR IDS instance respectively. This is similar to the Unified Communications Manager database that is used to maintain the CCM IDS instance.

The Cisco CAR DB service is activated on the publisher by default. The CAR DB instances are installed and actively run on the publisher, to maintain the CAR database. This network service is used only on the publisher and is not available on the subscribers.

Cisco Certificate Change Notification Service

This documentation update resolves CSCup84785.

The following content is omitted from the Platform Services section of the “Services” chapter in the *Cisco Unified Serviceability Administration Guide:*

Cisco Certificate Change Notification Service

This service keeps certificates of components like Tomcat, CallManager, and XMPP automatically synchronized across all nodes in the cluster. When the service is stopped and you regenerate certificates, you have manually upload them to Certificate Trust on the other nodes.

Cisco IP Phone Service Removed from CM Services

This documentation update resolves CSCur03499.

The Service groups and CM Services sections in *Cisco Unified Serviceability Administration Guide* mention Cisco IP Phone Service. This service has been removed from CM Services as IP Phone services is offered through the User Data Services (UDS) component starting Cisco Unified Communications Manager, Release 10.0(1).

Cisco SOAP-CallRecord Service

This documentation update resolves CSCup98302.

The following service is omitted from the “Services” chapter in the *Cisco Unified Communications Manager Serviceability Guide* and online help.

Cisco SOAP-CallRecord Service

The Cisco SOAP-CallRecord service runs by default on the publisher as a SOAP server, so that the client can connect to CAR database through the SOAP API. This connection happens through the use of the CAR connector (with a separate CAR IDS instance).

Delayed Initialization after IP Manager Assistant Service Restart

This documentation update resolves CSCus78713.

The following information is omitted from the "CTI Services" chapter in the *Serviceability Administration Guide*:

Expect a 12 to 15 minute delay after you restart the Cisco IP Manager Assistant service with a full resource load of 7000 users and 7000 phones.

Platform Administrative Web Service

This documentation update resolves CSCup84833.

The following service is incorrectly added to the " Feature Services" section in the *Cisco Unified Communications Manager Serviceability Guide* and online help. This service belongs to the "Network Services" section.

Platform Administrative Web Service

The Platform Administrative Web Service is a Simple Object Access Protocol (SOAP) API that can be activated on Cisco Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection systems to allow the PAWS-M server to upgrade the system.

Important Do not activate the Platform Administrative Web Service on the PAWS-M server.

Self Provisioning IVR Service

This documentation update resolves CSCum57057.

Although it appears in the *Cisco Unified Serviceability Administration Guide* and online help, the Self Provisioning IVR Service is unavailable in the **Alarm Configuration** window in Cisco Unified Serviceability.

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.

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.

SOAP-Diagnostic Portal Database Service

This documentation update resolves CSCuq22399.

The following service is omitted from the "Services" chapter in the *Cisco Unified Communications Manager Serviceability Guide* and online help.

SOAP-Diagnostic Portal Database Service

The Cisco Unified Real-Time Monitoring Tool (RTMT) uses the SOAP-Diagnostic Portal Database Service to access the RTMT Analysis Manager hosting database. RTMT gathers call records based on operator-defined filter selections. If this service is stopped, RTMT cannot collect the call records from the database.

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>**.

Minimize Disk Space utilized by Log Files

This documentation update resolves CSCva35260.

The following entry is omitted from the "Audit Log Configuration Settings" table in the *Cisco Unified Serviceability Administration Guide*.

Field	Description
Set to Default	The **Set to Default** button specifies the default values. It is recommended to set the audit logs to default mode unless it is required to be set to a different level for detailed troubleshooting. The **Set to Default** option minimizes the disk space utilized by log files.

System Error Messages

CSCvg70867 Documentation Defect Update

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
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

CSCvd71818 Documentation Defect Update

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

Reason Code	Description
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
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

Reason Code	Description
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
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

Reason Code	Description
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

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
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
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)

Reason Code	Description
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
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

Reason Code	Description
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

System Guide

Call Transfer to Hunt Pilot Restriction

This documentation update resolves CSCuw57732.

The following information is omitted from the “Phone Features” section in “Cisco Unified IP phones” chapter:

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.

Common Service Ports

This documentation update resolves CSCve02996.

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

Table 7: 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 *Cisco Unified Communications Manager System Guide*.

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.

Email IDs on the Active Directory Server

This documentation update resolves CSCur55902.

The following information is omitted from the “Directory Overview” in the *Cisco Unified Communications Manager System Guide*.

Note For the users that must be synchronized to the Cisco Unified Communications Manager database, their email ID fields on the active directory server must be unique or blank.

LDAP Directory Support

The "Configure LDAP Directory" topic in the *Cisco Unified Communications Manager System Guide, Release 10.0(1)* contains a list of supported LDAP directories. However, this list should include Microsoft Active Directory 2012 and Microsoft Lightweight Directory Services 2012 R1/R2.

The complete list of supported directories is as follows:

- Microsoft Active Directory 2003 R1/R2
- Microsoft Active Directory Application Mode (ADAM) 2003 R1/R2
- Microsoft Active Directory 2008 R1/R2
- Microsoft Lightweight Directory Services 2008 R1/R2
- Microsoft Active Directory 2012 R1/R2
- Microsoft Lightweight Directory Services 2012 R1/R2
- Sun One 6.x
- Sun Directory Services 7.0
- Oracle Directory Services Enterprise Edition 11gR1 (v11.1.1.5.0)
- OpenLDAP 2.3.39 & 2.4.x

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.

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.

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.

TAPI Developers Guide

Unsupported CTI Events from SIP Phones

This information resolves CSCur36240.

The *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager* and the *Cisco Unified TAPI Developers Guides for Cisco Unified Communications Manager* do not provide details on the following CTI events. These CTI events are not supported for SIP phones. Developers who are programming third party applications that invoke these CTI events should use SCCP phones.

- CallOpenLogicalChannelEvent
- CallRingEvent
- DeviceLampModeChangedEvent
- DeviceModeChangedEvent
- DeviceDisplayChangedEvent
- DeviceFeatureButtonPressedEvent
- DeviceKeyPressedEvent
- DeviceLampModeChangedEvent
- DeviceRingModeChangedEvent

TCP and UDP Port Usage Guide

Missing Information about TCP Port 22

This documentation update resolves CSCus05634.

The following entry is omitted from the "Intracluster Ports Between Cisco Unified Communications Manager Servers" table in the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager* :

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager Publisher	Unified Communications Manager Subscriber	22 / TCP	Cisco SFTP service. You must open this port when installing a new subscriber.

Missing Information about TCP Port 5555

This documentation update resolves CSCus26925.

The following entry is omitted from the " Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager" table in the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager* :

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	Cisco License Manager	5555 / TCP	Cisco License Manager listens for license requests on this port

Missing Information about Common Service Port 8006

This documentation update resolves CSCuy48628.

The following entry is omitted from the " Common Service Ports " table in the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager* :

From (Sender)	To (Listener)	Destination Port	Purpose
ILS Service Port		8006 / TCP	

Upgrade Guide

Disable or Postpone LDAP Synchronization During an Upgrade

This document update resolves CSCuq07331.

The following information is omitted from the "Preupgrade Tasks" chapter in the *Upgrade Guide for*

It is recommended that you disable or postpone the LDAP synchronization on Unified Communications Manager during an upgrade. If the synchronization is scheduled in for a time period which falls after the Unified Communications Manager upgrade and before the IM and Presence Service upgrade, then the result can negatively affect the IM and Presence Service if user changes occurred in this timeframe.

InterCluster Peer-User and Admin-CUMA Application User Roles Deprecated

The application user group roles InterCluster Peer-User and Admin-CUMA are deprecated from release 10.0(1). Any application users with these roles configured in releases 8.x or 9.x have the roles removed during an upgrade to any 10.x release. After the upgrade the administrator must configure appropriate roles for these users.

Note For intercluster to function correctly, the AXL user defined on the IM and Presence Service user interface (**Presence** > **Inter-Clustering**) must have a Standard AXL API Access role associated with it on the Unified Communications Manager application user page.

Unified CM 10.0 Upgrade Process Correction

This documentation update resolves CSCup31306.

In the Change Virtual Machine Configuration Specifications procedure, Step 6 ("Shut down the virtual machine") should be performed before Step 3 ("Change the configuration of the virtual machine").

Configuration and Administration Guide for IM and Presence Service

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.