Release notes for Cisco Unified Presence release 8.6(5)

June 11, 2013

These release notes describe requirements, restrictions, and caveats for Cisco Unified Presence Release 8.6(5).

Note To view the release notes for previous versions of Cisco Unified Presence, go to the following URL: http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html

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

Introduction

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

These release notes describe new features, requirements, restrictions, and caveats for Cisco Unified Presence Release 8.6(5). These release notes are updated for every maintenance release but not for patches or hot fixes.

Before you install Cisco Unified Presence, Cisco recommends that you review the "Related documentation" section on page 9 for information about the documentation available for Cisco Unified Presence.

System requirements

Hardware server requirements

Note For OVA template details and location, see http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Downloads_%28including_OVA/OVF_Templates%29#Cisco_Unified_Presence.

The Cisco Unified Presence system is a software product that is loaded onto a hardware server. The hardware server must meet the following requirements:

- One of the following server models:
  - Cisco 7800 Series Media Convergence Server (MCS) listed in the *Hardware and Software Compatibility Information for Cisco Unified Presence*. Go to Cisco.com for the latest information: http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

Note Cisco Unified Presence does not support MCS-xxxx-I1-IPC1 or MCS-xxxx-H1-IPC1 servers. However, a bridged upgrade is available to customers who need to migrate from any discontinued hardware, except for the following servers: MCS-7825-H1-IPC1, MCS-7825-I2-IPC1, MCS-7825-I1-IPC1, MCS-7825-I2-IPC2. For details about the unsupported hardware and the bridged upgrade, see the *Upgrade Guide for Cisco Unified Presence Release 8.6* here: http://www.cisco.com/en/US/products/ps6837/prod_installation_guides_list.html

  - Cisco-approved, customer-provided third-party server that is the exact equivalent of one of the supported Cisco MCS servers. Go to http://www.cisco.com/go/swonly.
  - Cisco Unified Computing System B-series blades or Cisco Unified Computing System C-series rack-mount servers. For information about these Cisco Unified Computing System servers, see the *Hardware and Software Compatibility Information for Cisco Unified Presence Release 8.x here:* http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html
- DVD-ROM drive
- Keyboard, mouse, and monitor

Note Additional server requirements, such as port and IP address requirements, are described in *Port Usage Information for Cisco Unified Presence.*

The Cisco Unified Presence installer checks for the availability of the DVD-ROM drive, sufficient hard drive and memory size, and sufficient CPU type and speed.

Cisco Unified Presence supports bridged upgrades from any of the following servers:

- MCS-7825-H2-IPC1
- MCS-7825-H2-IPC2
- MCS-7835-H1-IPC1
- MCS-7835-I1-IPC1
- MCS-7845-H1-IPC1
- MCS-7845-H2-IPC1 (only if each of the two disks has less than 72 GB of storage space, otherwise it is fully supported)
- MCS-7845-I1-IPC1

The bridged upgrade allows you to create a Disaster Recovery System backup on the discontinued hardware. You can then restore the DRS backup on supported hardware after you complete a fresh Cisco Unified Presence installation on the supported hardware. If you attempt an upgrade on discontinued hardware, Cisco Unified Presence displays a warning on the interface and on the CLI, informing you that Cisco Unified Presence only supports the functionality to create a DRS backup on this server.

Server software requirements

The Cisco Unified Presence server runs on the Cisco Linux-based operating system. This operating system is included with the application.

Related Topic

Installation and upgrade notes, page 6

Supported browsers

Use Microsoft Internet Explorer Version 6.0 or a later release, or Mozilla Firefox Version 3.0 or a later release, to access these interfaces: Cisco Unified Presence Administration, Cisco Unified Serviceability, and Cisco Unified Operating System Administration.

Note Cisco Unified Presence does not currently support Safari or Google Chrome on the Mac OS or Microsoft Windows.

How to use Hypertext Transfer Protocol over Secure Sockets Layer

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS), which secures communication between the browser client and the Apache Tomcat web server, uses a certificate and a public key to encrypt the data that is transferred over the Internet. HTTPS, which ensures the identity of the server, supports applications such as Cisco Unified Serviceability. HTTPS also ensures that the user sign-in password is transported securely over the web.

HTTPS for Internet Explorer

The first time you access Cisco Unified Presence Administration or other Cisco Unified Presence Secure Sockets Layer (SSL)-enabled virtual directories after a Cisco Unified Presence installation or upgrade, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must respond in one of the following ways:

- By selecting **Yes**, you select to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application: that is, until you install the certificate in the trusted folder.
- By selecting **View Certificate > Install Certificate**, you indicate that you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display every time you access the web application.
- By selecting **No**, you cancel the action. No authorization occurs, and you cannot access the web application. To access the web application, you must select Yes or install the certificate using the View Certificate > Install Certificate option.

Note The system issues the certificate using the hostname. If you attempt to access a web application using the IP address, the Security Alert dialog box displays, even though you installed the certificate on the client.

Saving the certificate to the trusted folder

You can save the CA Root certificate in the trusted folder, so the Security Alert dialog box does not display each time that you access the web application.

Step 1 Perform the required steps depending on the Internet browser you are using:

Table 1 Saving the certificate to the Trusted folder

If you are using...	Actions	Troubleshooting tips
Internet Explorer 6 or 8	**a.** Browse to the application on the Tomcat web server. **b.** Select **View Certificate** when the Security Alert dialog box displays. **c.** Select **Install Certificate** in the General pane of the Certificate dialog box. **d.** Select **Next** in the Certificate Import Wizard dialog box. **e.** Select **Place all certificates in the following store**. **f.** Select **Browse** adjacent to the Certificate store field. **g.** Browse to **Trusted Root Certification Authorities**. **h.** Select **OK**, then **Next**, and then **Finish**. **i.** Select **Yes** to install the certificate. **j.** Select **OK** after you receive a message stating that the import was successful. **k.** Select **OK** in the lower right corner of the Certificate dialog box. **l.** Select **Yes** to trust the certificate, so you do not receive the dialog box again.	• After you save the certificate to the trusted folder in Internet Explorer, the next time you browse to the server, ensure that you enter the fully qualified domain name (FQDN) of the server that is associated with the certificate. • You can verify that the certificate was installed successfully by selecting the Certificate Path tab in the Certificate pane.

Table 1 Saving the certificate to the Trusted folder (continued)

If you are using...	Actions	Troubleshooting tips
Internet Explorer 7	**a.** Browse to the application on the Tomcat web server. **b.** Select **Continue to this website (not recommended)** option to access the server. **c.** Select **View Certificate** when the Security Alert dialog box displays. **d.** Select **Install Certificate** in the General pane of the Certificate dialog box. **e.** Select **Next** in the Certificate Import Wizard dialog box. **f.** Select **Automatically select the certificate store** based on the type of certificate. **g.** Select **Next** and then **Finish**. **h.** Select **Yes** in the Security Warning dialog box. **i.** Select **OK** in the Certificate Import Wizard dialog box.	• After you save the certificate to the trusted folder in Internet Explorer, the next time you browse to the server, ensure that you enter the FQDN of the server that is associated with the certificate. • To verify that the trust store contains the imported certificate, select **Tools > Internet Options** in the Internet Explorer toolbar and select the Contents tab. Select **Certificates** and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list. • After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname or IP address or refresh or relaunch the browser. • You can verify that the certificate was installed successfully by selecting the Certification Path tab in the Certificate pane.
Netscape	**a.** Browse to the application using Netscape. **b.** Select one of the following radio buttons: • Accept this certificate for this session • Do not accept this certificate and do not connect • Accept this certificate forever (until it expires) **c.** Select **OK** in the Certificate Authority dialog box. **d.** Select **OK** in the Security Warning dialog box.	• After you save the certificate to the trusted folder in Netscape, the next time you browse to the server, ensure that you enter the FQDN name of the server that is associated with the certificate. • If you select **Do not accept this certificate and do not connect**, the application does not open. • To view the certificate credentials before installing the certificate, select **Examine Certificate**.

Installation and upgrade notes

Upgrade sequence

You must perform the Cisco Unified Presence Release 8.6(x) upgrade *before* you perform the Cisco Unified Communications Manager Release 8.6(x) upgrade. Cisco does not support Cisco Unified Presence 8.0(x) servers running with Cisco Unified Communications Manager Release 8.5 or 8.6.

Licensing requirements

If you upgrade from Release 7.0(x) to Release 8.6(x), you require a new software version license for *each* Cisco Unified Presence server in your deployment. You must order a separate software version license for each Cisco Unified Presence server. However, you need to upload the license to the first node in a cluster. For information about Cisco Unified Presence licensing modes and requirements, see the *Installation Guide for Cisco Unified Presence Release 8.6* here:

http://www.cisco.com/en/US/products/ps637/prod_installation_guides_list.html

You can run this release of Cisco Unified Presence on a VMware virtual machine deployed on approved Cisco Unified Computing server hardware. For information about supported servers, see *Hardware and Software Compatibility Information for Cisco Unified Presence Release 8.x*. For information about the VMware licensing requirements, see the License Activation for Cisco UC on UCS Docwiki here:

http://docwiki.cisco.com/wiki/License_Activation_for_Cisco_UC_on_UCS

Recommendations

Before you upgrade from Cisco Unified Presence Release 8.0(x), 8.5(x), or 8.6(x) to Release 8.6(5), Cisco *strongly advises* that you follow the recommended upgrade procedure in the *Upgrade Guide for Cisco Unified Presence Release 8.6* here:

http://www.cisco.com/en/US/products/ps6837/prod_installation_guides_list.html

Important notes

- Publisher node—Upgrade the Publisher node and switch the software to the new software release before you begin an upgrade and switch version on the Subscriber nodes. If the Cisco Unified Presence Administration GUI is operational on the Publisher node, it is safe to initiate an upgrade and switch version on the Subscriber node. Services on the Publisher will not start until the Subscribers are switched, restarted, and replication is successfully established on that cluster.
- High Availability User Support—Cisco Unified Presence Release 8.6(x) supports up to 45,000 Unified Communications mode users per cluster in a High Availability (HA) configuration across six nodes and up to 45,000 users per cluster in a non-HA configuration across three nodes. If, when you upgrade, you are left with a number of unsupported users, we recommend that you unlicense these surplus users on Cisco Unified Communications Manager before you perform the upgrade.
- Contact List Size—The default maximum value is 200; however you can configure this to a higher value, or configure 0 to set it to Unlimited. After you perform the upgrade, check that the contact list size for users has not reached the maximum value. If you have a large number of contacts per user, the number of users that a Cisco Unified Presence node supports is reduced.
- Platform Manager—You cannot use Platform Manager to upgrade to Cisco Unified Presence Release 8.6(5).

Upgrading to Cisco Unified Presence release 8.6(5)

Perform the following steps to upgrade from the following supported upgrade paths:

- Release 8.0(x) to Release 8.6(5)
- Release 8.5(x) to Release 8.6(5)
- Release 8.6(x) to Release 8.6(5)

Note Direct upgrades from Cisco Unified Presence Release 7.0(x) and earlier to Release 8.6(5) are not supported. You must first upgrade to another 8.x release, up to and including 8.6(3), and then perform a *Refresh Upgrade*. A Refresh Upgrade is significantly different from a Standard Upgrade. For more information, see the *Upgrade Guide for Cisco Unified Presence 8.6*. For more information about upgrading to Cisco Unified Presence Release 8.x, see the *Upgrade Guide for Cisco Unified Presence*: http://www.cisco.com/en/US/products/ps6837/prod_installation_guides_list.html.

Before you begin

- You can only download point releases of Cisco Unified Presence software from Cisco.com.
- Upgrades from 8.0(x) through to 8.6(3) require you to install a Cisco Options Package (COP) file on all nodes before you start the upgrade. Download the following COP file from Cico.com: `ciscocm.cup.refresh_upgrade_v<latest_version>.cop`

Procedure

Step 1 Go to http://www.cisco.com/upgrade.

Step 2 Enter your software contract number.

Step 3 Select the CUP<pre-upgrade release>-8-6-U-K9= option to order. If you do not see this option, contact your Cisco Account Team or Reseller to resolve your Contract issue.

Step 4 Go to http://www.cisco.com/cisco/software/navigator.html.

Step 5 Navigate to **Products > Voice and Unified Communications > Unified Communications Applications > Cisco Unified Presence > Cisco Unified Presence 8.6 > Unified Presence Server Updates**.

Step 6 Download the complete ISO file: UCSInstall_CUP_8.6.5.10000-12.sgn.iso.

Use an md5sum utility to verify that the MD5 sum of the final file is correct:
cfbb315123eeffad1dd769ef5aa82706 UCSInstall_CUP_8.6.5.10000-12.sgn.iso

Troubleshooting tips

You can upgrade the ISO image onto a remote server. Copy the ISO file (UCSInstall_CUP_8.6.5.10000-12.sgn.iso) to your FTP or SFTP server.

Related topic

Upgrade sequence, page 7

Related documentation

The complete Cisco Unified Presence documentation set, with the latest information for Release 8.6(x), is now available here on Cisco.com:

http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

To search for documentation on any given release, we recommend that you use the Custom Google search capability that was introduced in the last release.

For more information, see the *Deployment Guide for Cisco Unified Presence Release 8.6*:

http://www.cisco.com/en/US/products/ps6837/products_licensing_information_listing.html

New and changed information

The following sections describe new features and changes that are pertinent to Cisco Unified Presence Release 8.6(5). The sections may include configuration tips, information about users, and where to find more information.

- Enhanced Cisco Unified Presence deployment support, page 9
- Bulk rename of contact IDs, page 9

Enhanced Cisco Unified Presence deployment support

The enterprise-wide presence domain is no longer required to align with the DNS domain of any server. A Cisco Unified Presence deployment can have a common presence domain, while having nodes deployed across multiple DNS domains. If any Cisco Unified Presence node name is based on the hostname only, all Cisco Unified Presence nodes must share the same DNS domain. However, if all Cisco Unified Presence nodes within the deployment have a node name set to the FQDN or IP address for that node, the following deployment options are supported:

- Cisco Unified Presence clusters deployed in different DNS domain or subdomains
- Cisco Unified Presence nodes within a cluster deployed within different DNS domains or subdomains
- Cisco Unified Presence nodes within a cluster deployed in a DNS domain that is different to the associated Cisco Unified Communications Manager cluster

For more information, see the *Deployment Guide for Cisco Unified Presence*.

Bulk rename of contact IDs

The Cisco Unified Presence Bulk Administration Tool has been extended in Release 8.6(5) to support migrations where the SIP URI formats on Cisco Unified Presence and Lync/OCS/LCS differ. In Cisco Unified Presence Release 8.6(4) and earlier, you must change the SIP URI of all the migrating Lync/OCS/LCS users to match the Cisco Unified Presence SIP URI format before you migrate the first batch of users. From Cisco Unified Presence Release 8.6(5), you can change the SIP URI of migrating users just before each batch of users is migrated from Lync/OCS/LCS to Cisco Unified Presence. Cisco Unified Presence Bulk Administration Tool takes a CSV file with the list of migrated users as input and updates the contact lists for all users that have migrated users as contacts. For more information, see the *Partitioned Intradomain Federation Guide for Cisco Unified Presence*.

Important notes

The following section contains information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 8.6(5).

CPU spike causes database connection failure

Problem

The following Cisco Unified Presence interfaces can become inaccessible due to database connectivity problems. When you attempt to log in to the following applications, the login will appear to hang and will not complete:

- Cisco Unified Presence Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified End User Options

Cause

This condition affects Cisco Unified Presence running in a virtualized environment where the virtual machine (VM) on which Cisco Unified Presence is running has only one CPU. A large CPU spike on the Cisco Unified Presence server can cause the database to become inaccessible. You can verify that you are experiencing this issue by performing the following procedure:

Step 1 From the Cisco Unified Presence CLI, execute the following command to view the database log file:
`file view activelog /cm/log/informix/ccm.log`

Step 2 Check the log file for entries similar to the following:
`listener-thread: err = -25582: oserr = 0: errstr = : Network connection is broken.`

Solution

To resolve this issue, add an additional CPU to the VM on which Cisco Unified Presence is running.

Caveats

Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These release notes contain descriptions for the following:

- All severity level 1 or 2 bugs

- Significant severity level 3 bugs
- All customer-found bugs

You can search for specific bugs using the Cisco Software Bug Toolkit.

Before you begin

To access Bug Toolkit, you need the following items:

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

Procedure

Step 1 To access the Bug Toolkit, go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Sign in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the "Search for Bug ID" field, then select **Go**.

For information about how to search for bugs, create saved searches, and create bug groups, select **Help** on the Bug Toolkit page.

Resolved caveats

This section lists caveats that are resolved but that may be have been open in previous releases.

Bugs are listed in alphabetical order by component and then in numerical order by severity. Because defect status continually changes, be aware that this document reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access the Bug Toolkit (see Using Bug Toolkit, page 10).

Table 2 Resolved caveats for Cisco Unified Presence release 8.6(5)

Identifier	Severity	Component	Headline
CSCud41228	3	commonapi	Retrieving Login Status should not involve calls to Remote Nodes
CSCuc48394	3	config-agent	ConfigAgent hogs memory and CPU if binding to a port already in use
CSCuc62612	3	config-agent	Changing CUCM on CUP doesn't update proxy ACLs
CSCtz17304	3	cpi-appinstall	CUCM 8.6.2 doesn't clean /common/rpm-archive directory during RU
CSCtq56972	4	ctigw	CTIGW: Add protection code against core due to misconfigured Tel Uri
CSCue51167	3	customerutils	Migration Tool cannot export sip uri which include an apostrophe
CSCud61948	2	database	DRS restore failing on DB component - extra db chunks on dest deployment
CSCuc13886	3	database	Unable to Activate Services on CUP subscriber
CSCuc71396	3	database	nodename change from hostname to FQDN causes replication to break
CSCua02402	3	database	L2 upgrade failed on the full provisioned cluster with 45k users

Table 2 Resolved caveats for Cisco Unified Presence release 8.6(5) (continued)

Identifier	Severity	Component	Headline
CSCua60813	3	epe	Presence Engine core dump if IMDB service shut down on large system
CSCuc39002	3	epe	User receives error when sending IM, if PWS subscription for recipient
CSCue18666	3	epe	User_id change on AD causes contacts not to send availability
CSCue45984	3	epe	Presence Engine cored while handling calendar
CSCud22574	3	epe	Out of memory on startup due to large number of WinfoEventTable entries
CSCuc71516	4	epe	PE logs IM rejection make logging more descriptive
CSCue28127	3	esp	SIP Proxy user location lookup query can take 13 seconds
CSCuc35088	3	gui	Don't allow quotes in ldap profile search context field
CSCuc99206	3	gui	Unable to edit/delete CUPS Subcluster if it has # sign
CSCuc65107	3	gui	Install/Upgrade screen displays blank screen preventing upgrade
CSCuc88678	4	gui	CUPC 8.6.4 Presence Viewer Calendar Integration Incorrect
CSCud26765	4	gui	Remove Orative Logic from Presence Viewer
CSCuc28212	3	gui-serviceability	Serviceability page not accessible with SSO enabled after backup/restore
CSCtr36119	3	gui-troubleshooter	Exchange Server Status reports false positives
CSCuf61028	3	gui-troubleshooter	Troubleshooter reports unknown error when service account has no mailbox
CSCuc24056	3	intercluster	ICSA does not update trust store for tomcat certs
CSCud45321	3	intercluster	ICSA optimization of local copy is incorrect for pub/sub
CSCua29144	3	licensing	No licensing warning when grace period exists
CSCuc71494	4	pws	PWS CPU check log should be reduced to INFO level
CSCug29446	2	security	ASA self-signed certificate not functioning
CSCuc28694	3	security	SSO status is not correct after L2 upgrade from 8.6.4 SU2 to 8.6(5)
CSCuc95669	3	security	IPSec cannot be set up because ipsec-truststore cannot accept leaf certs
CSCud51156	3	security	SUB upgrade fails with FIPS enabled
CSCuc21848	4	security	CUPS Subject Alternate Name is not properly placed in the CSR
CSCud34859	3	selinux	Third-party LDAP Connection Troubleshooter test fails to run
CSCug21472	2	serviceability	DRS Restore Overwrites xcp_sequence table w/ Pub values on all Sub Nodes
CSCtz74208	3	serviceability	SNMP query unable to distinguish between services.
CSCue05820	3	serviceability	ReplWatcher Notifications fail as it uses local hostname instead of FQDN
CSCue16893	3	serviceability	Cisco OAM Agent Service not Listed in TLC IM_AND_Presence Services tab
CSCub43934	3	serviceability	CPU DoS During Malformed Packet Attack Against UDP SNMPRI Port
CSCuc28444	2	vos	DRS Failure: upload of signed XMPP certificates leaves invalid softlinks
CSCud45525	2	vos	Port CSCub14050 to Cisco Unified Presence due to Customer Found Defect on 8.6.4
CSCue30906	2	vos	Database replication won't set up in multinode deployment
CSCub42461	2	vos	Subscriber defined by hostname - IP address change failure

Table 2 Resolved caveats for Cisco Unified Presence release 8.6(5) (continued)

Identifier	Severity	Component	Headline
CSCuf78630	2	vos	perf.UCMPerf process prevents dbmon from binding to port 8001 for CNs
CSCud00228	3	vos	Update of Java and glibc libraries to match CUCM GGSG
CSCtx19301	4	vos	CUP subscriber report [utils diagnose test] incorrect error
CSCuc43524	2	xcp-router	CUP SDNS Deadlock when userid contains a space
CSCud14291	1	xcp-voslogger	After users log in Cisco UP XCP Authentication service stop working.
CSCuc41254	3	xcp-voslogger	logging not working in connection manager following binary rename

Open caveats

The caveats in the following table describe possible unexpected behavior in the latest Cisco Unified Presence release. These caveats may also be open in previous releases. Bugs are listed in alphabetical order by component and then in numerical order by severity.

Table 3 Open caveats for Cisco Unified Presence release 8.6(5)

Identifier	Severity	Component	Headline
CSCtw75780	3	bat	Some imported contacts' availability not showing when max contacts size set.
CSCtz47557	3	database	Update statistics timeout on rosters table during L2
CSCty85346	3	database	CLI 'dbreplication forcedatasyncsub' does not work on Cisco Unified Presence.
CSCtw94962	3	database	CUP support for over 4M roster entries per CUP server
CSCuc06375	4	database-tt	TimesTen install failure as part of COP file install
CSCue95139	3	epe	Users in Contact List lose presence if userid is changed
CSCuc50653	3	epe	Multi-Device DND State Transitions
CSCuf74738	3	epe	PEPeerNodeFailureAlarmMessage alerts seen regularly in RTMT
CSCty82743	4	epe	Presence Engine Core Dump during jabberd restart
CSCue35412	4	epe	PE Core on subscriber for CN from DBMon
CSCuf56468	4	epe	"Could not be delivered message" appears although message is received
CSCty41459	3	epe-privacy	[CUP]Unblock contact makes some other blocked contacts become unblocked
CSCud62757	3	esp	Not all SIP is encrypted when configuring secure SIP trunk to CUCM
CSCtu42689	4	esp	Phone presence not shown in CUPC when CUPS hostname starts with a number
CSCty29379	3	gui	CUP GUI not working when some services are restarted while SSO enabled
CSCty82764	3	gui	SSO logout screen not consistent
CSCue37852	3	gui	Repeatedly logged out trying to add a Backup Device on DRS GUI

Table 3 Open caveats for Cisco Unified Presence release 8.6(5) (continued)

Identifier	Severity	Component	Headline
CSCue72366	4	gui	CUPS Troubleshooter page showed error message for SIP Publish Model
CSCue39044	4	gui-admin	Admin GUI System Troubleshooter - Replication Watcher error misleading
CSCtj69153	5	gui-admin	Presence Viewer reports remote User as Local
CSCue87461	5	gui-admin	CUP Admin GUI Sort Feature Not Displaying Client Versions
CSCuf56559	4	gui-drs	GUI goes blank during DRS restore, Web locks up
CSCuf04522	4	gui-serviceability	guiRework on msg in changing Federation Routing CUP FQDN
CSCue58345	3	gui-troubleshooter	CUPS DB Troubleshooter reports errors on a working connection
CSCue11433	3	gui-troubleshooter	CUP should display a warning if the CUCM version is on 9 or greater
CSCue55553	3	gui-troubleshooter	System Troubleshooter slow on large scale test beds
CSCug28096	3	install	Sub Installation over WAN Fails - 3 different instances ver 8.6.4, 9.1.1
CSCue93395	3	intercluster	Subscriber deletes the root certificate, triggers CNs to delete other clusters
CSCts11780	5	licensing	“License Unit Report” only displays 1 unit when 2 sip proxy are running
CSCue67719	4	pws	mismatch between SOAP WSDL and server side limit of subscribe request
CSCuc39596	3	security	SSO enable fails with tomcat service not starting
CSCuf55909	3	security	PKI SSO: enabling SSO from CLI fails when users use UPN for Jabber
CSCuf93495	3	security	SUB upgrade from CLI fails when FIPS enabled
CSCug18764	3	security	Leaf certificates not able to be uploaded to tomcat-trust
CSCug34543	3	security	PKI CAC: oscp tomcat cert status cached in IE for variable periods
CSCug09157	3	security	PKI SSO: intermittent http 500, 403, bad cert error when sso enabled
CSCtz25566	3	security	HA can’t be enabled - version missing
CSCue54958	3	security	Enabling SSO fails after creating backup on SSO disabled CUP
CSCtt79854	3	serviceability	AlertCentral and CoreDumpFileFound alert properties XML parse error
CSCua21087	4	serviceability	XCP Router restart not bring processes up cleanly
CSCtz23921	3	serviceability	Pub fails to communicate with subscriber servm when enable/disable HA
CSCub74468	4	soap-interface	User cannot log in if their password finishes with a space
CSCuf65811	3	srm	Make SRM parameter defaults worst case for platform/OVA deployed
CSCtz03862	4	sync-agent	New changes made on CUCM cannot sync automatically to CUP
CSCuc26300	3	vos	Changing Node name halts access XCP Config Manager restart
CSCue03204	3	xcpauth	Auth Cores after manual PE and XCP shutdown
CSCug31825	3	xcp-connmgr	Perf: Excessive overhead in connection manager for getSSLContext
CSCty14182	3	xcp-jsm	XMPP login failures due to bind errors at scale.
CSCtz23657	4	xcp-jsm	No warning if user tries to IM user on failed node on another cluster
CSCug28771	3	xcp-router	DB query for groups table update to include user_id
CSCuc11276	3	xcp-sipgw	SIP Federation Connection Manager core
CSCue04106	3	xcp-sipgw	SIP S2S core after manual PE and XCP shutdown
CSCub53720	4	xcp-sipgw	Core dump on SIP federation manager caused a reboot of the service

Documentation updates

For the latest versions of all Cisco Unified Presence documentation, go to http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

Updates were made to the following documents:

Online Help updates

Bulk administration tool contact rename

This topic was added to describe the Bulk Administration Tool Contact Rename feature.

Cluster topology configuration

This topic was updated to specify that node names must be defined by the FQDN or IP address.

Deployment Guide for Cisco Unified Presence Release 8.6

The *Deployment Guide for Cisco Unified Presence Release 8.6* was updated with the following new sections:

- DNS Domain Configuration
- Configuring the DNS domain associated with a Cisco Unified Communications Manager cluster for Release 8.6(5) and later
- Bulk Rename of Contact IDs

The following chapters or sections were enhanced to provide more detailed information:

- Configuring Single Sign-On—Updated for enhanced usability. Note that procedural content for OpenAM configuration on Linux platforms has been removed.
- Node Name Recommendations—Updated with new recommendations for 8.6(5) and later.

- Replacing the Default Presence Domain after Installation—Updated to include a procedure for Release 8.6(4) and earlier and a procedure for Release 8.6(5) and later.
- Node Name Value for Intercluster Deployments—Updated with recommendations for Release 8.6(4) and earlier and Release 8.6(5) and later.

Serviceability Configuration and Maintenance Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6

The *Serviceability Configuration and Maintenance Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6* was updated to indicate that end user configuration of IM chat rooms (ad hoc and persistent) is now logged by various components of the Cisco Unified Presence application.

Cisco Unified Operating System Maintenance Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6

The *Cisco Unified Operating System Maintenance Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6* was updated to include Single Sign-On support for the Cisco UP Client Profile Agent (Cisco Jabber).

Installation Guide for Cisco Unified Presence Release 8.6

The postinstallation task to change the Cisco Unified Presence node name to a resolvable value has been updated with information for releases earlier than Cisco Unified Presence Release 8.6(5) and for Release 8.6(5) and later.

Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6

The following updates have been made:

- Added a new chapter detailing user migration planning.
- Updated the workflow for user migration to include two new procedures:
  - Verify Lync/OCS/LCS SIP URI Format for Migrating Users
  - Rename Contact IDs in Cisco Unified Presence Contact Lists
- Added a detailed description of the new Bulk Administration Tool Contact Rename Tool

Changing the IP Address, Hostname, Domain Name, and Node Name for Cisco Unified Presence Release 8.6.5

This is a new document that describes how to change the server IP address, hostname, domain name, or node name for Cisco Unified Presence Release 8.6(5).

Obtaining documentation and submitting a service request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.
