ReadMe for Cisco Unified Presence Release 8.6(4)SU2

September 23, 2012

These release notes describe requirements, restrictions, and caveats for Cisco Unified Presence Release 8.6(4)SU2.

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

Contents

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 amongst 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(4)SU2. 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 10 for information about the documentation available for Cisco Unified Presence.

System Requirements

Hardware Server Requirements

Note Cisco Unified Presence Release 8.6(4)SU2 requires 4 GB of RAM, except for the 500 user and Business Edition 6000 OVA deployments, which require 2 GB of RAM.

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 of the 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 rackmount 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 presence of the DVD-ROM drive, sufficient hard drive and memory sizes, 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 72GB of storage space, otherwise it is fully supported)
- MCS-7845-I1-IPC1

The bridged upgrade allows you to create a DRS 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 (HTTPS)

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), 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 via the web.

HTTPS for Internet Explorer

The first time you (or a user) access Cisco Unified Presence Administration or other Cisco Unified Presence 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 via 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 and 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. **a.** Select **Place all certificates in the following store**. **b.** Select **Browse** adjacent to the Certificate store field. **c.** Browse to **Trusted Root Certification Authorities**. **d.** Select **OK**. **e.** Select **Next**. **f.** Select **Finish**. **g.** Select **Yes** to install the certificate. **h.** Select **OK** after you receive a message stating that the import was successful. **i.** Select **OK** in the lower, right corner of the Certificate dialog box. **j.** 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.** Browse **Next**. **h.** Select **Finish**. **i.** Select **Yes** in the Security Warning dialog box. **j.** 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 T**ools > 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 re-enter 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) • Select **OK** in the Certificate Authority dialog box. • 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

System Upgrade

Supported Upgrade Paths to Cisco Unified Presence Release 8.6(4)SU2

Cisco Unified Presence supports the following software upgrade paths to Release 8.6(4)SU2:

Table 2 Supported Upgrade Paths

Supported Upgrade Paths from Cisco Unified Presence...	Installation Instructions
Release 8.0(x), 8.5(x), or 8.6(x) to 8.6(4)SU2	**Before You Begin** Upgrades from 8.0(x) through to 8.6(1) require you to install a COP file on all nodes prior to starting the upgrade. Download the following COP file from Cico.com: `ciscocm.cup.refresh_upgrade_v<latest_version>.cop` Perform these steps to proceed with the upgrade: 1. Go to http://www.cisco.com/upgrade. 2. Enter your software contract number. 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 and/or Reseller to resolve your Contract issue. 4. Go to http://www.cisco.com/cisco/software/navigator.html. 5. Navigate to Products > Voice and Unified Communications > Unified Communications Applications > Cisco Unified Presence > Cisco Unified Presence 8.6 > Unified Presence Server Updates. 6. Download the complete ISO file: UCSInstall_CUP_8.6.4.12900-1.sgn.iso

Note Direct upgrades from Cisco Unified Presence Release 7.0(x) and earlier to Release 8.6(4)SU2 are not supported. You must first upgrade to an earlier 8.x release of Cisco Unified Presence. 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.

Upgrade from Cisco.com

Cisco does not support downloading major Cisco Unified Presence software releases from Cisco.com, for example, Cisco Unified Presence Release 8.0. From Cisco.com you can download upgrade-only software images that are used to upgrade from a previous major software release to a subsequent software maintenance release or point release of Cisco Unified Presence. For example, you can download Cisco Unified Presence Release 8.0(2) or Cisco Unified Presence Release 8.6(4)SU2 from Cisco.com.

To download this software, go to http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240. You must have an account on Cisco.com to access the Software Center. The images posted at the Software Center require existing installations of Cisco Unified Presence.

Related Topics

- Supported Upgrade Paths to Cisco Unified Presence Release 8.6(4)SU2, page 7
- The Latest Software Upgrades for Cisco Unified Presence on Cisco.com, page 8

The Latest Software Upgrades for Cisco Unified Presence on Cisco.com

Perform the following steps to access the upgrade file for Cisco Unified Presence release 8.5(x) to 8.6(4)SU2.

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(1) require you to install a COP file on all nodes prior to starting the upgrade. Download the following COP file from Cico.com: `ciscocm.cup.refresh_upgrade_v<latest_version>.cop`

Procedure

Step 1 Download the UCSInstall files from Cisco Connection Online.

Step 2 Use an md5sum utility to verify that the MD5 sum of the final file is correct:

611bdaee7eab20214b7d2326083d4c5f UCSInstall_CUP_8.6.4.12900-1.sgn.iso

Troubleshooting Tips

You can upgrade the ISO image onto a remote server. Copy the ISO (UCSInstall_CUP_8.6.4.12900-1.sgn.iso) to your FTP or SFTP server.

Related Topics

- System Upgrade, page 6
- Upgrade from Cisco.com, page 7

Additional Installation and Upgrade Considerations

- Perform Cisco Unified Presence 8.6(x) Upgrade Before Cisco Unified Communications Manager 8.6(x) Upgrade, page 9
- Licensing Requirements for Release 7.0(x) to 8.6(x) Upgrades, page 9
- Software Licensing Requirements for VMware, page 9
- Recommendations for Release 8.0(x), 8.5(x), or 8.6(x) to 8.6(4)SU2 Upgrades, page 9
- Platform Manager is Not Supported, page 10

Perform Cisco Unified Presence 8.6(x) Upgrade Before Cisco Unified Communications Manager 8.6(x) Upgrade

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 for Release 7.0(x) to 8.6(x) Upgrades

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

Software Licensing Requirements for VMware

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 for Release 8.0(x), 8.5(x), or 8.6(x) to 8.6(4)SU2 Upgrades

Before you upgrade from Cisco Unified Presence Release 8.0(x), 8.5(x), or 8.6(x) to Release 8.6(4)SU2, 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

Note Direct upgrades from Release 7.x and earlier to 8.6(4)SU2 are not supported. You must first upgrade to another 8.x release 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*.

Important Notes

- Publisher node—upgrade the publisher node and switch the software to the new software release prior to initiating 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. There are special considerations that need to be taken into account when upgrading to Release 8.6(4)SU2. Cisco recommends that you refer to the *Upgrade Guide for Cisco Unified Presence 8.6* before you proceed with upgrading.

Note 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 users per cluster in a High Availability (HA) configuration across 6 nodes and up to 45,000 users per cluster in a non-HA configuration across 3 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 value. 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 is Not Supported

Platform Manager (PM) cannot be used to upgrade to Cisco Unified Presence Release 8.6(4)SU2.

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 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

Support for Microsoft Lync for Partitioned Intradomain Federation was added in this release. You can find more about this feature in the "Partitioned Intradomain Federation document for 8.6(4)SU2" document. See Related Documentation chapter.

Several defects have been resolved. For more information, see Resolved Caveats, page 13.

Important Notes

The following sections contain information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 8.6(4)SU2:

CPU Spike Causes Database Connection Failure

Problem

The following Cisco Unified Presence interfaces can become inaccessible due to database connectivity problems. When attempting to login 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 on 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.

IPSec cannot be set up because ipsec-truststore cannot accept leaf certs

Symptom

IPSec between Cisco Unified Presence nodes or between Cisco Unified Presence and Cisco Unified Communication Manager nodes cannot be setup when using Signed certificates that is a leaf certificate. When an administrator tries to upload a signed certificate thats a leaf certificate, will fail with the warning "Only CA and intermediate CA certificate can be uploaded".

Conditions

Cisco Unified Presence version is 8.6.4.12900-2 ->Cisco Unified Presence 8.6.(4) release Service Update 2 Signed Certificate is a leaf certificate and not an intermediate CA certificate.:

Workaround

A) Cisco Unified Presence Cluster has been Upgraded but not switched to 8.6.4.12900-2

1. Follow the relevant OS Administration guide to upload IPsec certificates on all nodes which you wish to setup IPsec.
2. Follow the relevant OS Administration guide to Configure Ipsec policy between nodes which you wish to setup IPsec.
3. Follow the relevant OS Administration guide to Verify Ipsec is working between all nodes which you wish to setup IPsec.
4. Switch all Cisco Unified Presence nodes to 8.6.4.12900-2
5. Follow the relevant OS Administration guide to Verify Ipsec is working between all nodes which you wish to setup IPsec.

B) Cisco Unified Presence Cluster has been Upgraded & switched to 8.6.4.12900-2

1. Switch back all your Cisco Unified Presence nodes to the older version. Refer the appropriate guide to understand procedure & impacts of switching back to the older version. Verify that all nodes has been successfully switched back before moving to next step.
2. Follow the relevant OS Administration guide to upload IPsec certificates on all nodes which you wish to setup IPsec.
3. Follow the relevant OS Administration guide to Configure Ipsec policy between on all nodes which you wish to setup IPsec.
4. Follow the relevant OS Administration guide to Verify Ipsec is working between all nodes which you wish to setup IPsec.
5. Switch all Cisco Unified Presence nodes to 8.6.4.12900-2
6. Follow the relevant OS Administration guide to Verify Ipsec is working between all nodes which you wish to setup IPsec.

Note Workaround is not applicable if:
1) This is a fresh install of Cisco Unified Presence of version 8.6.4.12900-2.
2) Cisco Unified Presence Nodes has to be enabled to FIPs mode when running at version 8.6.4.12900-2. Do not tryout this workaround if your intention is to enable FIPs mode while running in 8.6.4.12900-2 version.

Caveats

Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These ReadMe file contains descriptions of the following:

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

You can search for problems by 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 the Using Bug Toolkit, page 12).

Table 3 Resolved Caveats for Cisco Unified Presence Release 8.6(4)SU2

Identifier	Severity	Component	Headline
CSCub66064	3	bat	Unable to BAT contacts into CUPS when Contact Domain begins with Number
CSCua28273	4	commonapi	Certificate Import Tool reports error for manual CUCM ipsec certificate
CSCua33835	3	config-agent	Offline messages are not moved when user is assgned to different node
CSCty64210	4	config-agent	SIP Proxy Static Routes checks are incorrectly case-sensitive
CSCtq51761	6	config-agent	Config agent prints the password for the DB user
CSCtq51326	6	config-agent	Config Agent Performance enhancement requirements for DB queries
CSCua73880	3	ctigw	CUPS 8.6.4 is causing core dump with RCC
CSCta42149	6	ctigw	RCC feature fails for users with apostrophe (') in their OCS sing-in ID
CSCub13154	6	customerutils	Migration Utilities - Support for Lync
CSCub74794	6	customerutils	Export tool reports users with 0 contacts as not having been processed
CSCua12285	3	database	Boot up after switch back hanging at 'Starting cupOnL2BootInitd'
CSCtz64227	3	database	Carriage return control characters in db data can cause upgrade failure
CSCub90171	2	database-imdb	PE and TTSoft core in CUPS 8.6.4
CSCua62944	4	database-imdb	IMDB SQL parser will fail if SQL keywords are queried as column values
CSCua21220	4	database-imdb	PEIDStoIMDBDatabaseSyncError - block contact
CSCuc14008	4	database-imdb	IMDB copyFromPeer error logged as EMERGENCY, alarm raised at PE startup
CSCua21072	3	epe	Multiple Presence Engine core dumps
CSCuc21396	3	epe	PE Manual Presence bug with IMDB
CSCua89930	3	esp	CUP: Permanent CPU DoS Following TCP Flood on ESP port 5060
CSCtz83598	3	esp	SIP Retransmits result in shared memory exhaustion
CSCtz96324	3	gui	Auditor user does not have exclusive permission to audit log files
CSCty82764	3	gui	SSO logout screen not consistent
CSCty06969	4	gui	Tomcat Attribute "secure" error on startup
CSCtz06790	3	gui-accessibility	When admin locks user on CUCM, user can always access GUI pages with SSO
CSCua28898	3	gui-admin	CUPS ACL Address Pattern Does Not Allow CIDR Notation
CSCtz50782	3	gui-admin	Incorrect CUCM Hostname can cause Subscriber Install to fail
CSCua14744	6	gui-admin	Jabber Presence DND
CSCub74433	6	gui-admin	GUI changes for Lync Intradomain Federation
CSCtz82910	2	intercluster	Unreachable ICSA peer can take down IDS
CSCub94915	3	intercluster	Regenerated self signed SUB cert not seen by IC peer

Table 3 Resolved Caveats for Cisco Unified Presence Release 8.6(4)SU2

Identifier	Severity	Component	Headline
CSCtz62315	3	intercluster	ICSA handling errors for CNs being sent
CSCua81803	3	intercluster	ICSA should handle two hostnames resolving to same IP address
CSCty85505	4	intercluster	Intercluster Sync Agent throws exception cleaning up obselete users
CSCuc06339	3	security	SSO does not work after upgrade if CUP Admin app was not enabled
CSCua07173	4	security	No warning provided for inappropriate certificates upload to truststore
CSCub96425	4	security	upload a leaf cert signed by inter CA as a trust cert, no warning msg.
CSCub80046	3	serviceability	CUP Syslog Messages Not Showing in Remote Syslog
CSCtz49498	3	serviceability	UNKNOWN_PARAMNAME:PEAlarmMessage alerts in syslog from Presence Engine
CSCts61745	3	serviceability	Syslog messages dropped when Router debug logging enabled
CSCty19323	4	serviceability	Tomcat hangs during an L2 upgrade
CSCtr46570	6	serviceability	Serviceability: RTMT counter for SRM status
CSCtz69301	6	serviceability	Admin Friendliness for the Number of Logon Sessions Parameter
CSCub92633	4	soap-interface	IMDB: CUP Client Profile Agent Trace shows incorrect result
CSCub92597	4	soap-interface	IMDB: CUPC user fails to login after re-configuring end user setting
CSCtz26078	3	vos	OpenSSH: DSA/DSS connections does not work in FIPS mode
CSCua52799	3	xcp-connmgr	XCP Connection Manager stuck in Paused state.
CSCub82470	3	xcp-jcore	CUP not presenting intermediate certs over Client XMPP interfaces
CSCub34625	3	xcp-router	XCP Router: AddressResolver should prioritize by availability
CSCtz43848	3	xcp-s2s	EFT S2S Core during dialback validation
CSCua57986	3	xcp-textconf	Text Conference doesn't drop packets when TC queue size gets too big

Open Caveats

The caveats in Table 4 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 4 Open Caveats for Cisco Unified Presence Release 8.6(4)SU2

Identifier	Severity	Component	Headline
CSCtw75780	3	bat	Some imported contacts' presence not showing when max contacts size set
CSCua19295	6	bat	CUPS request for ability to pre populate contacts for CUPC and Jabber
CSCtz96671	3	cupxcpconfig	Incorrect restart notification for sub's XMPP fed connection manager
CSCtz88557	3	database	CPU spike causes database connection failure
CSCua02402	3	database	L2 upgrade failed on the full provisioned cluster with 45k users
CSCto77824	3	database	Users have inconsistent presence after Cisco Unified Presence Upgrade
CSCty85346	3	database	CLI 'dbreplication forcedatasyncsub' doesn't work on CUP
CSCtz38528	3	database	L2 upgrade of PUB node in fully provisioned 45k System taking 27hrs
CSCtz26163	3	epe	PE core on startup when Calandering GW is configured
CSCtz55120	3	epe	Possible memory leak on soak test run
CSCtz99702	3	epe	Relogin of Jabber casuses error impacting presence composition
CSCua68248	6	epe	Add NTLMv2 support to CUP Exchange Calendaring
CSCty29379	3	gui	CUP GUI not working when some services are restarted while SSO enabled
CSCuc35088	3	gui	Don't allow quotes in ldap profile search context field
CSCtz31616	3	gui-platform	Upgrade lock is not being released. Can't restart/switch version via GUI
CSCtr36119	3	gui-troubleshooter	Exchange Server Status reports false positives
CSCua29144	3	licensing	No licensing warning when grace period expires

Table 4 Open Caveats for Cisco Unified Presence Release 8.6(4)SU2

Identifier	Severity	Component	Headline
CSCts53870	3	oamagent	Delay in writing pe_cfg.xml upon L2 causes PE to start in bad state
CSCtz25566	3	security	HA can't be enabled - version missing
CSCuc95669	3	security	IPSec cannot be set up because ipsec-truststore cannot accept leaf certs
CSCtz10360	3	serviceability	Server status not reliably retrieved on Cluster Topology page
CSCtz23921	3	serviceability	Pub fails to communicate with subscriber servm when enable/disable HA
CSCtt79854	3	serviceability	AlertCentral and CoreDumpFileFound alert properties XML parse error
CSCts28606	3	serviceability	"UNKNOWN_ALARM" alerts sent to remote syslog server on router restart
CSCtz74208	3	serviceability	SNMP query unable to distinguish between services
CSCub39612	4	srm	SRM status logging is not readable for debugging HA issues
CSCuc26300	3	vos	Changing Node name halts access XCP Config Manager restart
CSCty14182	3	xcp-jsm	XMPP login failures due to bind errors at scale

Documentation Updates

Following updates were made to documents for Cisco Unified Presence Release 8.6(4)SU2:

Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6

- Title of the document “Integration Guide for Configuring Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6 and Microsoft LCS/OCS” has changed to “Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6”.
- New chapter for configuring Microsoft Lync for Partitioned Intradomain Federation.
- Several updates to the remaining chapters all concerning support for Microsoft Lync.

Deployment Guide for Cisco Unified Presence Release 8.6

- Section “Configuring Single Sign-On” has been changed.

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

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.