Release Notes for Cisco Unified Presence Release 8.0

November 16, 2010

These release notes describe requirements, restrictions, and caveats for Cisco Unified Presence Release 8.0(1) up to and including Cisco Unified Presence Release 8.0(4).

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/sw/voicesw/ps556/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 Unified Personal Communicator 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 8.0(x). These release notes are updated for every maintenance release but not for patches or hot fixes.

Before you install Cisco Unified Presence, we recommend 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, page 2
- Server Software Requirements, page 3
- Supported Browsers, page 3

Hardware Server Requirements

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   Note, for Release 8.0(x), that Cisco Unified Presence does not support MCS-xxxx-I1-IPC1 or MCS-xxxx-H1-IPC1servers. However, a bridged upgrade is available to customers who need to migrate from any of the discontinued hardware to supported hardware. For details of the unsupported hardware and the bridged upgrade, see the *Installation and Upgrade Guide for Cisco Unified Presence.*

    - 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.
- 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.

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 Topics

- Installation and Upgrade Notes, page 3

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 Communications Operating System Administration.

> **Note** Cisco Unified Presence does not currently support Safari or Google Chrome on MAC or Windows operating systems.

Installation and Upgrade Notes

- New System Installation, page 3
- System Upgrade, page 4
- The Latest Software Upgrades for Cisco Unified Presence on Cisco.com, page 5

New System Installation

For new installations, you must order the Cisco Unified Presence system software and adhere to licensing requirements. To order the software, go to http://www.cisco.com/en/US/ordering/index.shtml or contact your Cisco sales representative.

Each Cisco Unified Presence shipment comes with an installation DVD, which is required for all new installations of a major software release of Cisco Unified Presence, for example, Cisco Unified Presence Release 8.0(1). The Cisco Unified Presence operating system and application software is installed from the installation DVD. For new installations of the Cisco Unified Presence 8.0(1) application, use the DVD that indicates Cisco Unified Presence 8.0(1) Installation.

Related Topics

- Software Licensing Requirements for 7.0(x) to 8.0(x) Upgrades, page 8

- Software Licensing Requirements for VMWare, page 8
- Inconsistent Behavior with Cisco Unified Presence Evaluation License, page 20

System Upgrade

- Supported Upgrade Paths to Cisco Unified Presence Release 8.0(x), page 4
- Upgrade from Cisco.com, page 5

Supported Upgrade Paths to Cisco Unified Presence Release 8.0(x)

Cisco Unified Presence supports the following software upgrade paths to Release 8.0(x):

Supported Upgrade Paths from Cisco Unified Presence...	Installation Instructions
Release 1.0(x) to 8.0(x)	Direct upgrades from Cisco Unified Presence Release 1.0(x) to Release 8.0(x) are not supported. You must first upgrade to Release 7.0(x) of Cisco Unified Presence. For more information about upgrading to Release 7.0(x), see the *Release Notes for Cisco Unified Presence Release 7.0(x)* here on Cisco.com: http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html
Release 6.0(x) to 8.0(x)	Direct upgrades from Cisco Unified Presence Release 6.0(x) to Release 8.0(x) are not supported. You must first upgrade to Release 7.0(x) of Cisco Unified Presence. For more information about upgrading to Release 7.0(x), see the *Release Notes for Cisco Unified Presence Release 7.0(x)* here on Cisco.com: http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html
Release 7.0(x) to 8.0(x)	Upgrades from Release 7.0(x) to Release 8.0(x) require the UCSInstall_CUP_*.sgn.iso file. Perform these steps to order the "Installation and Upgrade (7.0(x) to 8.0.(x))" upgrade DVD and acquire the .isofile as part of your Cisco Unified Presence order: 1. Go to http://www.cisco.com/upgrade. 2. Enter your software contract number. 3. Select the CUP7-8-0-U-K9= option to order. If you do not see the CUP7-8-0-U-K9= option, contact your Cisco Account Team and/or Reseller to resolve your Contract issue. 4. Install the "Installation and Upgrade (7.0(x) to 8.0.(x))" upgrade DVD that Cisco provides.

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(1). 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 point release of Cisco Unified Presence. For example, you can download Cisco Unified Presence Release 8.0(2) 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

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

Before You Begin

You can only download point releases of Cisco Unified Presence software from Cisco.com.

Accessing the Upgrade File for Cisco Unified Presence Release 8.0(1) to 8.0(2)

Because of its size, the original UCSInstall ISO file, UCSInstall_CUP_8.0.4.10000-4.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_CUP_8.0.2.10000-30.sgn.iso_part1of2
- UCSInstall_CUP_8.0.2.10000-30.sgn.iso_part2of2

Procedure

Step 1 Download the two UCSInstall files from Cisco Connection Online.

Step 2 Depending on your operating system, execute one of the following commands in the CLI to reunite the two parts of the file:

OS	Command - copy and paste to CLI
Unix/Linux	cat UCSInstall_CUP_8.0.2.10000-30.sgn.iso_part1of2 UCSInstall_CUP_8.0.2.10000-30.sgn.iso_part2of2 > UCSInstall_CUP_8.0.2.10000-30.sgn.iso
Windows	COPY/B UCSInstall_CUP_8.0.2.10000-30.sgn.iso_part1of2+UCSInstall_CUP_8.0.2.10000-30.sgn.iso_part2of2 UCSInstall_CUP_8.0.2.10000-30.sgn.iso

Step 3 Use an md5sum utility to verify that the MD5 sum of the final file is correct.

- e7489d29b58cf1da5d24c7c41438f4b8 UCSInstall_CUP_8.0.2.10000-30.sgn.iso

Troubleshooting Tips

You can upgrade the ISO image onto a remote server as an alternative to using the upgrade DVD. After you reunite the two files as documented in this procedure, copy the ISO (UCSInstall_CUP_8.0.2.10000-30.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- New System Installation, page 3

Accessing the Upgrade File for Cisco Unified Presence Release 8.0(1) to 8.0(3)

Because of its size, the original UCSInstall ISO file, UCSInstall_CUP_8.0.3.10000-4.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_CUP_8.0.3.10000-4.sgn.iso_part1of2
- UCSInstall_CUP_8.0.3.10000-4.sgn.iso_part2of2

Procedure

Step 1 Download the two UCSInstall files from Cisco Connection Online.

Step 2 Depending on your operating system, execute one of the following commands in the CLI to reunite the two parts of the file:

OS	Command - copy and paste to CLI
Unix/Linux	cat UCSInstall_CUP_8.0.3.10000-4.sgn.iso_part1of2 UCSInstall_CUP_8.0.3.10000-4.sgn.iso_part2of2 > UCSInstall_CUP_8.0.3.10000-4.sgn.iso
Windows	COPY/B UCSInstall_CUP_8.0.3.10000-4.sgn.iso_part1of2+UCSInstall_CUP_8.0.3.10000-4.sgn.iso_part2of2 UCSInstall_CUP_8.0.3.10000-4.sgn.iso

Step 3 Use an md5sum utility to verify that the MD5 sum of the final file is correct.

- 130a3bf2f5d1a2e9ab0595a8427fa232 UCSInstall_CUP_8.0.3.10000-4.sgn.iso

Troubleshooting Tips

You can upgrade the ISO image onto a remote server as an alternative to using the upgrade DVD. After you reunite the two files as documented in this procedure, copy the ISO (UCSInstall_CUP_8.0.3.10000-4.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- New System Installation, page 3

Accessing the Upgrade File for Cisco Unified Presence Release 8.0(1) to 8.0(4)

Because of its size, the original UCSInstall ISO file, UCSInstall_CUP_8.0.4.10000-5.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_CUP_8.0.4.10000-5.sgn.iso_part1of2
- UCSInstall_CUP_8.0.4.10000-5.sgn.iso_part2of2

Procedure

Step 1 Download the two UCSInstall files from Cisco Connection Online.

Step 2 Depending on your operating system, execute one of the following commands in the CLI to reunite the two parts of the file:

OS	Command - copy and paste to CLI
Unix/Linux	cat UCSInstall_CUP_8.0.4.10000-5.sgn.iso_part1of2 UCSInstall_CUP_8.0.4.10000-5.sgn.iso_part2of2 > UCSInstall_CUP_8.0.4.10000-5.sgn.iso
Windows	COPY/B UCSInstall_CUP_8.0.4.10000-5.sgn.iso_part1of2+UCSInstall_CUP_8.0.4.10000-5.sgn.iso_part2of2 UCSInstall_CUP_8.0.4.10000-5.sgn.iso

Step 3 Use an md5sum utility to verify that the MD5 sum of the final file is correct.

- 836236bca62cab262af187351d96f7d7 UCSInstall_CUP_8.0.4.10000-5.sgn.iso

Troubleshooting Tips

You can upgrade the ISO image onto a remote server as an alternative to using the upgrade DVD. After you reunite the two files as documented in this procedure, copy the ISO (UCSInstall_CUP_8.0.4.10000-5.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- New System Installation, page 3

Additional Installation and Upgrade Considerations

- Perform Cisco Unified Presence 8.0(x) Upgrade Before Cisco Unified Communications Manager 8.0 (x) Upgrade, page 8
- Software Licensing Requirements for 7.0(x) to 8.0(x) Upgrades, page 8
- Software Licensing Requirements for VMWare, page 8
- Recommendations for Release 7.0(x) to 8.0(x) Upgrades, page 8
- Recommendations for Release 7.0(x) to 8.0(x) Intercluster Upgrades, page 9

Perform Cisco Unified Presence 8.0(x) Upgrade Before Cisco Unified Communications Manager 8.0 (x) Upgrade

You must perform the Cisco Unified Presence Release 8.0(x) upgrade *before* you perform the Cisco Unified Communications Manager Release 8.0(x) upgrade. Cisco does not support Cisco Unified Communications Manager Release 8.0(x) running Cisco Unified Presence Release 7.0(x).

Software Licensing Requirements for 7.0(x) to 8.0(x) Upgrades

If you upgrade from Release 7.0(x) to 8.0(x), you require a new software version license for *each* Cisco Unified Presence server cluster in your deployment. You must order a separate software version license for each Cisco Unified Presence sever cluster. However, you only need to upload the license to the first node in a cluster. For information on Cisco Unified Presence licensing modes and requirements, see the *Deployment Guide for Cisco Unified Presence.*

Related Topics

Inconsistent Behavior with Cisco Unified Presence Evaluation License, page 20

Software Licensing Requirements for VMWare

This release of Cisco Unified Presence also allows you to run VMWare on a Cisco Unified Presence server. For more information on the VMWare licensing requirements, see the *Installation and Upgrade Guide for Cisco Unified Presence*.

Related Topics

Support for VMWare on Customer Deployments, page 14

Recommendations for Release 7.0(x) to 8.0(x) Upgrades

Before you upgrade from Cisco Unified Presence Release 7.0(x) to Release 8.0(x), we *strongly advise* that you follow the recommended upgrade procedure in the *Deployment Guide for Cisco Unified Presence*.

These are important notes that you should be aware of: (and are described in detail in the Deployment Guide):

- Cisco Unified Presence Release 8.0(x) supports 15,000 users per cluster. 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.

- If you have 15,000 users across six nodes in an active standby deployment, you can delete the unused nodes from the topology, either before or after the upgrade. We recommend that you delete unused nodes because they increase the serviceability overhead of your deployment.

- If you deploy the active/standby user assignment model in Cisco Unified Presence Release 7.0(x), and you upgrade to Cisco Unified Presence Release 8.0(x), where the active/standby model no longer supports failover, we recommend that you redistribute (rebalance) your users across the cluster.

- If you have 5000 users across six nodes in a balanced deployment, after you upgrade you can either move your users to three nodes and delete the unused nodes, or retain the deployment as is.

- After the upgrade, on each subsequent node you must restart the Presence Engine service once the database replication is active on the node. Run the "utils dbreplication runtimestate" CLI command (on the publisher or subsequent node) to check if the database replication is active on a node. If database replication is active on all nodes, the output lists all the nodes and the replication setup value for each node is two.

- The default value for the maximum number of contacts 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.

- After you perform the upgrade, request that all Cisco Unified Personal Communicator users in the local and remote cluster sign out, and sign back into the application.

Related Topics

Recommendations for Release 7.0(x) to 8.0(x) Intercluster Upgrades

Before you perform an intercluster upgrade from 7.0(x) to 8.0(x), we *strongly recommend* that you follow the intercluster upgrade procedure described in the intercluster chapter of the *Deployment Guide for Cisco Unified Presence*.

These are important notes that you should be aware of: (and are described in detail in the Deployment Guide)

- Before you perform the software upgrade, we highly recommend that you turn off (deactivate) the Cisco UP Presence Engine service in the local Cisco Unified Presence cluster. If you intend to upgrade all clusters to Release 8.0(x), you should turn off (deactivate) the Cisco UP Presence Engine on all clusters until you complete the intercluster upgrade in your intercluster deployment.

- To allow Cisco Unified Presence to reestablish the presence subscriptions with remote contacts in both the local and the remote cluster, you must reestablish the intercluster router-to-router connections (by restarting the Cisco UP XCP Router) before you turn on the Cisco UP Presence Engine. Until the roster migration is complete, local users will not see the availability status of remote contacts, and remote contacts will not see the availability of their contacts belonging to the local cluster.

- You may experience high CPU (possibly for several hours) while the Cisco UP Presence Engine attempts to reestablish any presence subscriptions with remote contacts.

- Presence subscriptions to remote contacts will not work for users who have reached their contact list size limit on the local or remote cluster.

- Cisco Unified Presence has a maximum limit on the number of SIP remote contacts that can be active at one time. This maximum value changes based on platform type (see the *Deployment Guide* for platform details). If you intend to leave an intercluster peer on Release 7.0(x), and you enable the Cisco UP XCP SIP Federation service, you may exceed this limit depending on the number of remote contacts on the 7.0(x) peer clusters. If you exceed the limit, Cisco Unified Presence will not process the remaining contacts.

Related Topics

Limitations and Restrictions

Table 1 contains a list of caveats, now in Closed state, that describe possible unresolved behavior (limitations) in the latest Cisco Unified Presence release. These caveats may also be open in previous releases. Bugs are listed in order of severity and then in alphanumeric order by bug identifier.

Table 1   Closed Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCsz06312	3	xcp	TC deadlock during shutdown after a load test
CSCtd92272	2	xcp-jsm	XCP services stopping after the XCP router was restarted for IC testing
CSCte29296	3	xcp-r2r	full-mesh out-of-memory failure on 7825s with 24 nodes networked

Related Documentation

The complete Cisco Unified Presence documentation set, with the latest information for Release 8.0(x), is now available for administrators 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 with this release. See Support for Google Custom Search from Cisco Unified Presence Interfaces, page 14.

New and Changed Information

For information about all available features and benefits, see the data sheet for Cisco Unified Presence at http://www.cisco.com/en/US/products/ps6837/products_data_sheets_list.html.

- About Cisco Unified Presence Release 8.0(1), page 10
- About Cisco Unified Presence Release 8.0(2), page 15

About Cisco Unified Presence Release 8.0(1)

The following sections describe new features and changes that are pertinent to Cisco Unified Presence, Release 8.0(1). The sections may include configuration tips for the administrator, information about users, and where to find more information.

- Copyright Information, page 11
- Support for Enterprise Instant Messaging including Point-to-Point IM and Group Chat, page 11
- Support for Regulatory Compliance Logging of Instant Messages and Group Chat, page 11
- Support for External Database Integration, page 12
- Support for Interdomain Federation with Third-Party XMPP Servers, page 12
- Support for Third-Party XMPP Clients Contact Search of Corporate LDAP Directory, page 12
- Personalized vCard Support, page 13
- Certificate Import Tool Security Enhancement, page 13

Copyright Information

Open source and third-party licenses govern portions of Cisco Unified Presence Release 8.0(1) software. For more information and acknowledgements of copyright, see the *Licensing Information for Cisco Unified Presence* at the following URL:

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

Support for Enterprise Instant Messaging including Point-to-Point IM and Group Chat

Cisco Unified Presence Release 8.0(1) supports Instant Messaging (IM) capability across the enterprise. This feature provides:

- Point-to-Point IM between SIP and XMPP clients

- Multi-device IM sessions—IMs initially fork to all of the devices that a user is signed into and subsequently to the single device from which the user responds.

- Group chat— Multiple users can exchange IMs in both temporary (ad-hoc) chat rooms and permanent (persistent) chat rooms. Note that group chat is an XMPP-only feature and that an external database is required for the permanent chat feature.

- Chat server aliases—Aliases enable administrators to create a unique address for each chat node so that users (in any domain) can search for specific chat rooms on specific nodes and join those rooms.

Related Topics
- Limitation with Privacy Settings on Third-Party XMPP Client, page 23
- Federation Group Chat Issue with GoogleTalk, page 29

Support for Regulatory Compliance Logging of Instant Messages and Group Chat

To support compliance regulations, Cisco Unified Presence Release 8.0(1) logs the records of the following IM activities in a single cluster, intercluster, or federated network configurations:

- Point-to-point messages

- Group chat including ad-hoc, or temporary chat messages, and permanent chat messages.

Two methods of regulatory compliance logging are available:

- Native compliance—Cisco Unified Presence uses an inherent Message Archiver component for logging messages to the external database. An external database is required for the native compliance feature.

- Support for external third-party provided compliance solutions—Supported clients include Cisco clients such as Cisco Unified Personal Communicator 7.0(x); third-party XMPP clients, and other third-party clients used in federated networks.

Support for External Database Integration

The native compliance logging and permanent group chat features in this release of Cisco Unified Presence require a remote database. The external database is PostgreSQL, Release 8.3x. The external database requirements differ depending on which feature you deploy on Cisco Unified Presence. For more information, see the *Database Setup Guide for Cisco Unified Presence.*

Related Topics

External Database Considerations, page 20

Support for Interdomain Federation with Third-Party XMPP Servers

This release allows Cisco Unified Presence users in one enterprise domain to exchange presence information and Instant Messaging (IM) with users in a foreign domain as follows:

- Federation with IBM Sametime 8.2 and 8.5 users, WebEx Connect users, GoogleTalk users and Cisco Unified Presence 8.0(1) users (in another domain) occurs over the standard Extensible Messaging and Presence Protocol (XMPP).

For SIP federation, version 8.3 of the Cisco Adaptive Security Appliance (ASA) is now supported.

Related Topics

- WebEx Connect (Version 6) Client Issues, page 29
- Federation Issues with IBM Sametime, page 28
- Federation Issues with IBM Sametime, page 28
- Cisco Unified Personal Communicator 7.0(x) Receives a Watcher INFO Popup Until the Contact or Domain is Added to the Privacy list, page 27
- Federation Group Chat Issue with GoogleTalk, page 29

Support for Third-Party XMPP Clients Contact Search of Corporate LDAP Directory

In this release, you can configure the LDAP corporate directory server to process contact search queries from third-party XMPP clients and return the results to the client. First, you configure the LDAP server. Then, complete the LDAP settings that allow Cisco Unified Presence to successfully perform contact search for XMPP clients.

Related Topics

Known Implications for Third-Party LDAP Server Configuration when using Mozilla Firefox on a MAC Operating System, page 26

Personalized vCard Support

With this release of Cisco Unified Presence, administrators can optionally enable retrieval of vCards from the corporate LDAP directory. If enabled, this feature allows third-party XMPP clients to search for and view their own vCard and vCards from other users. Clients, however, cannot update corporate LDAP-based vCards.

If this feature is disabled, vCards are stored locally in the "generic" table in the IDS database and XMPP clients can search for, retrieve and update their own vCard, and retrieve their contacts' vCards.

Certificate Import Tool Security Enhancement

The Certificate Import Tool on Cisco Unified Presence Release 8.0(1) simplifies the process of installing trust certificates on Cisco Unified Presence. The tool allows you to specify the host and port of a peer server, download the certificate chain from that server and automatically import the certificates to Cisco Unified Presence. The Certificate Import Tool attempts to install missing certificates automatically. Note, however, that there are circumstances where you may still need to manually download the missing certificates from the peer server and upload these certificates in Cisco Unified Operating System Administration.

Related Topics

Time Zone Synchronization Enhancement

Cisco Unified Presence Release 8.0(1) maintains correct and current time for any given time zone. You do not need to manually manage the update process. After you install Cisco Unified Presence Release 8.0(1), and after any subsequent time zone change event, Cisco contacts you to let you know that you can download a COP file (ciscocm.dst-updater.YYYYv-.el4.7..3.cop) to install on the servers in your Release 8.0(1) cluster. This file updates the time zone information automatically.

In the preceding file name example, "YYYY" represents the release year of the COP file, and "v" specifies the file version number.

New Services and Alarm Integration in Cisco Unified Serviceability Interface

To support the new features in this release, the Cisco Unified Serviceability interface includes a wide range of Cisco Unified Presence XCP services. Note that there is a requirement to restart many of these services after administrator changes. For more information see the Important Notes section of these release notes.

In addition, this release of Cisco Unified Presence includes new XCP alarms that collect information on the status of XCP components and services.

Related Topics

Additional Application Programmer Interfaces (APIs)

This release of Cisco Unified Presence introduces additional APIs including a BOSH interface on the Cisco Unified Presence server and a Jabberwerx SDK. The SDK is provided along with examples that inform you how to use the core SDK and the interface components. Consult the Cisco Developer Community for supported Cisco Unified Presence interfaces at the following URL:

http://developer.cisco.com/web/cdc/home;jsessionid=B2EE8D3CDB73A709AC8F88349ACD28.liferay-portal

Support for VMWare on Customer Deployments

You can install Cisco Unified Presence Release 8.0(1) on a VMWare virtual machine once you adhere to the specific licensing requirements, and hardware and software requirements for VMWare support. The installation procedure is largely the same as a Cisco Unified Presence installation on a physical server, with some documented exceptions. For information on the supported and recommended VMWare platforms, see the *Installation and Upgrade Guide for Cisco Unified Presence* for this release.

Related Topics

- Location of Virtual Machine Templates (OVA Templates) on Cisco.com, page 17
- Microsoft Office Communicator Remote Call Control Performance on VMWare, page 25
- DRS Restore to a Smaller Virtual Machine Fails, page 25

Support for Google Custom Search from Cisco Unified Presence Interfaces

Cisco Unified Presence Release 8.0(1) allows targeted search capability of Cisco Unified Presence documentation to provide more direct access to technical information from these interfaces:

- Cisco Unified Presence Administration
- Cisco Unified Operating System Administration
- Disaster Recovery System

You can customize your search and filter the results based on the software release.

Support Status for High Availability Deployments

If the primary server fails in this release of Cisco Unified Presence, users will *not* fail over to a back-up (standby) node and will, therefore, lose all instant messaging and presence capability. This release of Cisco Unified Presence does not provide a High Availability (HA) deployment option.

Note that the three modes of HA sync agent dispersal - None, Balanced, Active/Standby - remain integrated in the Cisco Unified Presence Administration interface for this release. However, this user assignment capability does not mean that HA is provided. If you upgrade from Release 7.0(x) to 8.0(1), and have Active/Standby mode enabled, consider reassigning your users because this release of Cisco Unified Presence ignores any standby node that you may have provisioned. If you configure Active/Standby mode and you do not rebalance your users, Cisco Unified Presence 8.0(x) does NOT use the standby node and therefore, there is no failover protection support to the backup node.

Related Topics

Recommendations for Release 7.0(x) to 8.0(x) Upgrades, page 8

Support Status for Cluster Over WAN Deployments

In Cisco Unified Presence Release 8.0(1), you cannot disperse subclusters geographically over the WAN. This release does not support Clustering over WAN for intracluster and intercluster deployments.

Support Status for Cisco Unified Personal Communicator Release 7.0(x)

This software release supports the Cisco Unified Personal Communicator 7.0(x) client for backward compatibility purposes. Note that presence and IM exchanges between Cisco Unified Presence and the Cisco Unified Personal Communicator 7.0(x) client occur over the SIP/SIMPLE -based interfaces.

Related Topics

About Cisco Unified Presence Release 8.0(2)

The following sections describe new features and changes that are pertinent to Cisco Unified Presence, Release 8.0(2). The sections may include configuration tips for the administrator, information about users, and where to find more information.

Support for Cisco Adaptive Security Appliance (ASA)

Cisco Unified Presence Release 8.0(x) supports Cisco Adaptive Security Appliance (ASA) Version 8.3(0).

Support for Cisco Unified Personal Communicator 8.0

This software release supports the Cisco Unified Personal Communicator 8.0 client. Cisco Unified Personal Communicator is a multi-media application that provides instant access from your desktop to integrated audio calls, enterprise instant messaging, visual voicemail, your corporate directory, video, and web conferencing. Cisco Unified Personal Communicator also provides an intuitive user interface, wide-band audio, and high-definition video.

Important Notes

About Cisco Unified Presence Release 8.0(1)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 8.0(1).

- Cisco Unified Personal Communicator 7.0(x) Receives a Watcher INFO Popup Until the Contact or Domain is Added to the Privacy list, page 27
- Federation Issues with IBM Sametime, page 28
- Federation Group Chat Issue with GoogleTalk, page 29
- WebEx Connect (Version 6) Client Issues, page 29
- Install Fails Due to Server Name Issue, page 29

Support for Cisco UCS B-Series Blade Servers

The Cisco Unified Presence Release 8.0(1) documentation contains support for Cisco UCS B-Series Blade servers. This support is contingent on, and aligns with, the announcement of support for Cisco UCS B-Series Blade servers for the Cisco Unified Communications 8.0(1) solution.

Service Restart Requirement for XMPP-related Administrator Changes

If you make a configuration change that impacts a Cisco Unified Presence XCP service in Cisco Unified Presence Administration, be aware that you may need to restart one or more services for your changes to take effect. Cisco Unified Presence Release 8.0(1) notifies you when you must restart XCP services via system alerts in the Cisco Unified Presence Administration interface.

Note that Cisco Unified Presence automatically restarts all active XCP services if you restart the Cisco Unified Presence XCP router. For more information, see the *Deployment Guide for Cisco Unified Presence*.

Location of Virtual Machine Templates (OVA Templates) on Cisco.com

A virtual machine template defines the configuration of a virtualized server. Open Virtualization Format (OVF) is an open standard for packaging and distributing virtual appliances and other software to be run on virtual machines. Files in this format have the extension *.ova. Therefore, virtual machine templates are sometimes called OVA templates or OVA files.

The configuration of a Cisco Unified Presence virtual machine must match a supported virtual machine template.

Perform the following procedure to obtain the virtual machine template for Cisco Unified Presence.

Procedure

Step 1   Select this URL in your browser:
http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

Step 2   If your browser prompts you to do so, type your Cisco.com User Name: and Password: in the text fields, then select **Log In**.

Step 3   Select **Unified Communications Applications > Cisco Unified Presence > Cisco Unified Presence Version 8.0**.

Step 4   Select the **Unified Presence Server (CUPS) Updates** link.

Step 5   In the Latest Releases folder, select the 8.0(1) link.

Step 6   Select **Download Now** for the OVA template that you require. Follow the prompts and provide the required information to download the software.

Step 7 When the Download Cart window displays, select the **Readme** link to view the release information for the virtual machine template.

What To Do Next

See the *Installation and Upgrade Guide for Cisco Unified Presence* for the import procedure.

Related Topics

For additional information on Unified Communications Virtualization, go to the DocWiki:

http://cisco.com/go/uc-virtualized

Intercluster Upgrades to Cisco Unified Presence Release 8.0(1)

For more information, see the Additional Installation and Upgrade Considerations section of these release notes.

Related Topic

Recommendations for Release 7.0(x) to 8.0(x) Intercluster Upgrades, page 9.

Intercluster Sync Agent Repeatedly Synchronizes with Remote Clusters

Problem

Known issues in the Intercluster Sync Agent cause the ICSA to fully synchronize with remote clusters whenever end user-to-phone associations are changed. This issue can cause a Presence Engine core, high CPU processing and other issues to occur in large deployments.

Cause

This condition occurs in a multi-cluster Cisco Unified Presence network.

Solution

To fix this issue, you must:

1. Download this COP file - ciscocm.cup_80_patch.cop.sgn - from here on Cisco.com:

    http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

2. Select **Cisco Unified Operating System Administration > Software Upgrades > Install/Upgrade** to apply the COP patch file.

Cisco Unified Presence XCP Services Stop After an XCP Router Start or Restart

Problem

Cisco UP XCP feature services may stop shortly after you start (or restart) the XCP router. The Cluster Topology window and Feature Services window show that the XCP router remains active while the Cisco UP XCP Authentication Service and the Cisco UP XCP Connection Manager stop.

Cause

This condition occurs, typically, in a large intercluster network with many nodes. Services stop after you start or restart the XCP router.

Solution

1. To preempt this problem, first start the XCP router on all nodes in the local cluster *before* you start the remaining XCP feature services.

2. If the problem occurs when the XCP Router is still running while the XCP Authentication Service and XCP connection manager have stopped, stop the XCP router. The router may take some time to stop but it is important to verify that the router is actually in Stopped state before you proceed further. Once the router has stopped, implement these steps to correct the problem. On all nodes in the local cluster:

   a. Stop the Cisco UP XCP Counter Aggregator on each node.

   b. Start (or restart) the Cisco UP XCP Router on each node.

   c. Restart the Cisco UP XCP Counter Aggregator on each node.

   ✎
   Note After you complete these steps on all nodes in the local cluster, you may start the remaining XCP feature services if they are not already running.

   d. Repeat this procedure in remote clusters if the problem also occurs there.

Troubleshooting Log Files for New Cisco Unified Presence XCP Services

The table below lists the Cisco Unified Presence XCP services introduced with this release, and provides the corresponding configuration and log files for each service:

Cisco Unified Presence XCP Service	Log Files - located under epas/trace/…	Relevant Configuration Files - located under /usr/local/xcp/...
Cisco UP XCP Router	*xcp/log/rtr-jsm-_*.log*	global.xml, jabber.xml, jsm-.xml
Cisco UP XCP Connection Manager	*xcp/log/client-cm-_*.log*	cm-.xml
Cisco UP XCP Web Connection Manager	*xcp/log/web-cm-2_*.log*	cm-2.xml
Cisco UP XCP SIP Federation Connection Manager	*xcp/log/sip-cm-3_*.log*	cm-3.xml
Cisco UP XCP XMPP Federation Connection Manager	*xcp/log/xmpp-cm-4_*.log*	cm-4.xml
Cisco UP XCP Text Conference Manager	*xcp/log/txt-conf-_*.log*	tc-.xml
Cisco UP XCP Directory Service	*xcp/log/dir-svc-_*.log*	jds-.xml
Cisco UP XCP Message Archiver	*xcp/log/msg-arc-_*.log*	ma-.xml
Cisco UP XCP Authentication Service	*xcp/log/auth-_*.log*	auth-.xml
Cisco UP XCP Counter Aggregator	*xcp/log4j/cntr-aggr_*.log*	/usr/local/xcp-svc/conf/XcaConfig.xml

Known Issues with Cisco Unified Personal Communicator 7.0(2) and Cisco Unified Presence 8.0(1) Integration

Although this release of Cisco Unified Presence supports integration with Cisco Unified Personal Communicator 7.0(x) clients, there are caveats that apply if you integrate Cisco Unified Personal Communicator Release 7.0(2) with Cisco Unified Presence Release 8.0(1).

Below is the list of functionality that is not supported with this specific integration. You cannot:

1. Enter a custom domain in the Create New Contact window. You must select from a list of federated domains specified on the Cisco Unified Presence server.

2. Send IMs to a contact when they are offline.

3. Add self to the contact list or subscribe to self-presence.

SIP Remote Contact Limit

Cisco Unified Presence has a maximum limit on the number of SIP remote contacts that can be active at one time. This maximum value changes based on platform type. If you leave an intercluster peer running Release 7.0(x), you may exceed this limit depending on the number of remote contacts on the 7.0(x) peer clusters. Similarly, if you wish to federate Cisco Unified Presence Release 8.0(1) with another SIP domain, you may exceed this limit depending on the number of remote contacts in your federated deployment. If you exceed the limit, Cisco Unified Presence will not process the remaining contacts.

You can configure the pre-allocated SIP stack memory value on Cisco Unified Presence. Select **Cisco Unified Presence Administration > System > Service Parameters > Cisco UP XCP SIP Federation Connection Manage**r, and configure the Pre-allocated SIP stack memory (bytes) value.

For more information on the SIP subscription limits for each platform type, see the intercluster chapter of the D*eployment Guide for Cisco Unified Presence*.

External Database Considerations

When you deploy an external database, consider the following issues:

- We highly recommend that the specification of the hardware platform is the same as the connected Cisco Unified Presence server. If you run an external database on an inferior hardware specification to the Cisco Unified Presence server, it may cause performance issues on Cisco Unified Presence.

- When you enable the Compliance or Permanent Chat archiving features on Cisco Unified Presence, the external database can consume disk space quickly and completely fill. It is necessary to have a strategy in place to perform routine database maintenance tasks such as those referenced in the PostgreSQL documentation here: http://www.postgresql.org/docs/8.4/static/maintenance.html

  Failure to implement this policy may lead to failures of the Message Archiver (MA) and Text Conference (TC) components on Cisco Unified Presence over time. The PostgreSQL documentation provides additional information on tasks such as Monitoring Disk Usage and other strategies for database management.

Inconsistent Behavior with Cisco Unified Presence Evaluation License

Problem

After a fresh installation of Cisco Unified Presence, the system defaults to Evaluation mode for 90 days. If, during this trial period, you use an Evaluation license to access Cisco Unified Presence Release 8.0(1), the following inconsistent behavior may occur:

- The Cisco Unified Presence Administration interface will show all users to be licensed for Cisco Unified Presence and Cisco Unified Personal Communicator even if those users do not have the license capability assigned in Cisco Unified Communication Manager.

- As a result, a user will be able to authenticate and connect to Cisco Unified Presence for Instant Message (IM) and presence capabilities. However, Cisco Unified Communication Manager will not publish phone presence requests unless those users are licensed from Cisco Unified Communication Manager.

Cause

This condition occurs when an Evaluation license is used to access Cisco Unified Presence in the 90-day evaluation period following a fresh installation.

Solution

Applying a permanent (Production mode) license to Cisco Unified Presence is the best way to preempt this problem. Users should upload the permanent Cisco Unified Presence server license and ensure that Cisco Unified Presence user license capability is assigned in Cisco Unified Communications Manager.

Note that Cisco will provide Cisco Unified Presence and Cisco Unified Personal Communicator licenses to all users during the evaluation period, irrespective of their actual license capability assigned in Cisco Unified Communication Manager.

Certificate Naming Conventions and Troubleshooting Information

The table below outlines new and changed certificates by name.

Certificate	Certificate Name	Notes
XMPP	cup-xmpp	Both XMPP and XMPP S2S certificates share the same trusted certificate store: cup-xmpp-trust
XMPP S2S	cup-xmpp-s2s	
SIP	• cup • cup-trust	• Called sip in previous releases. • Called sip-trust in previous releases.
Presence Engine	• cup • cup-trust	• Called presenceengine in previous releases. • Called presenceengine-trust in previous releases.
Exchange	cup-trust	Called presenceengine-trust in previous releases.
Third-party CA-signed certificate (Microsoft OCS server)	• cup • cup-trust	• Called sip in previous releases. • Called sip-trust in previous releases.

If you experience any issues with certificate management, check the following logs:

- Cisco UP Intercluster Sync Agent
- IPT Platform CertMgr Logs

Cisco Unified Personal Communicator Parameters Not Configurable in Cisco Unified Presence Administration

Some of the parameters that display in the Release 8.0(1) Cisco Unified Presence Administration interface are specific to the Cisco Unified Personal Communicator 8.0(1) client. This client release is not currently supported, so you cannot configure the following list of parameters.

- Audio Profile Configuration (select **Application > CUPC > Audio Profile**).

- CCMCIP Profile Configuration (select **Application > CUPC > CCMCIP Profile**).

- Cisco Unified Personal Communicator Configuration (select **Application > CUPC > Settings /** CUPC 8.0 Settings).

- Voicemail Profile Configuration (select **Application > CUPC > Voicemail Profile /** CUPC 8.0 Settings).

- Voicemail Profile Configuration (select **Application > CUPC > User Settings /** CUPC 8.0 Settings).

Contacts Management and User-Facing Changes in Client Behavior

If you upgrade from release 7.0(x) to Cisco Unified Presence Release 8.0(1), your lists of contacts will synchronize to the 8.0(1) server and its SIP and XMPP clients. However, note these caveats:

- You must sign out and sign in again to Cisco IP Phone Messenger for the contacts list synchronization to take effect. Contacts list do not automatically synchronize on Cisco IP Phone Messenger from other clients.

- Empty groups are not managed in the database and do not synchronize until you add a contact to that group. Until you add a contact:

  – Empty groups created by any client are invisible to any other client until you add a contact to it. Additionally, Empty groups are not managed in the server-side database.

  – Empty groups created in Cisco Unified Personal Communicator do not survive if you sign in again.

End User Data on Cisco Unified Presence May be Deleted During Legacy Cisco Unified Communications Manager Server Migration

Loss of contacts on Cisco Unified Presence may occur if you upgrade your Cisco Unified Communications Manager hardware from legacy hardware servers to a higher release, under these *specific* circumstances. Consider this migration scenario:

1. There is an existing Cisco Unified Communications Manager Release 7.0(x) and an existing Cisco Unified Presence Release 7.0(x) server.

2. The Cisco Unified Communications Manager Release 7.0(x) server cannot be directly upgraded to Cisco Unified Communications Manager Release 8.0(1) because the existing hardware does not support Cisco Unified Communications Manager Release 8.0(1).

3. You perform a DRS backup of Cisco Unified Communications Manager Release 7.0(x), install the same version of Cisco Unified Communications Manager Release 7.0(x) on the new hardware, and then perform a DRS restore on the new hardware from the backup of the old system.

4. During the backup and restore operations, you encounter some issues.

5. You decide to change course and perform a fresh installation of Cisco Unified Communications Manager Release 8.0(1) on the new hardware, configure the system manually, and synchronize the users again from the LDAP server.

6. At some later point, you upgrade the Cisco Unified Presence server from Release 7.0(x) to Release 8.0(1) and point Cisco Unified Presence to the new Cisco Unified Communications Manager Release 8.0(1).

Known Issue

When Cisco Unified Communications Manager Release 8.0(1) synchronizes new users from LDAP, it generates a unique id value for each end user (the pkid field in the database). Therefore, the Cisco Unified Communications Manager 7.0(x) and Cisco Unified Communications Manager 8.0(1) versions have different pkid values for users with the same userid (for example, 'chrisd').

When Cisco Unified Presence moves from one Cisco Unified Communications Manager server to the other, all the users from the old Cisco Unified Communications Manager server are deleted, and a new set of users, from the new Cisco Unified Communications Manager, are created. When the old users are deleted, all their associated information such as contact details are also deleted.

Limitation with Privacy Settings on Third-Party XMPP Client

Problem

You cannot customize your privacy settings to allow and block specific types of XMPP presence stanzas on Cisco Unified Presence.

Example: User A, who is logged into a third-party XMPP client, manipulates his privacy list to allow User B to see IMs but not presence information. After User A sends the privacy list update to the Cisco Unified Presence server, User B is still able to view and exchange IMs and presence information

Cause

This condition occurs because privacy policy on Cisco Unified Presence is designed to enable an allowed user to view presence information and exchange IMs; a blocked user cannot view presence information or exchange IMs. Users cannot configure permutations of block/allow functionality for presence information and IMs.

Solution

No workaround exists.

OpenLDAP Authentication of XMPP Clients Fails if DNS Not Used

Problem

Certificates are issued with a Fully Qualified Domain Name (FQDN), which openLDAP uses to match against the LDAP server that you want to connect to as part of the verification process. If you do not have DNS enabled in your network, however, you are prompted to enter an IP address (not the FQDN) on the LDAP authentication web page (select **System > LDAP > LDAP Authentication**). Because the uploaded certificate uses the FQDN and the web page uses an IP address, a mismatch occurs and openLDAP is not able to connect to the LDAP server.

Cause

This condition occurs if you do not enable DNS in your network.

Solution

We recommend that you use DNS.

Presence Subscription Approval in Multiple Clients May Cause Contacts to be Added to Multiple Groups

Problem

When the user approves the same presence subscription request in multiple clients, it may cause the contact to be added to multiple groups because each client uses a different default group. This is a client-side issue.

Cause

The user approves the same subscription request in multiple clients when the:

1. auto-authorization is off.

2. user signs in to multiple clients.

Solution

Delete the contact from one or more groups (if desired).

International Characters Break Cisco Unified Personal Communicator 7.0(x) and Cisco Unified Presence Interoperability

Problem

If a user of a Cisco Unified Personal Communicator 7.0(x) client has a user name that contains international characters, their attempt to sign in fails with a authentication denied error.

Cause

This condition occurs when user names with international characters attempt to sign in to the Cisco Unified Personal Communicator client.

Solution

Change the user name on Cisco Unified Communication Manager to remove the conflicting characters

Changes to Hostname and IP Address Breaks Database Replication

Problem

After a hostname change, database replication within a cluster breaks and the Cisco UP XCP router does not start. The changed hostname may or may not have propagated to the rest of the cluster. This same issue also applies (potentially) to IP address changes if nodes are identified by IP address in the topology.

Cause

This condition typically occurs after a name change on a subscriber node. It can also occur after a name change on a publisher node.

Solution

Sign in to the Command Line Interface (CLI) for each node in the cluster, and enter these commands:

1. Run **utils dbreplication stop** on the subscriber node. Do this for each subscriber node, one at a time, and wait for completion.

2. Run **utils dbreplication stop** on the publisher node, and wait for completion.

3. Run **utils dbreplication dropadmindb** on the subscriber node. Do this for each subscriber node, one at a time, and wait for completion.

4. Run **utils dbreplication dropadmindb** on the publisher node.

5. On the publisher ONLY, run **utils dbreplication clusterreset**.

6. After the successful return of the previous command, restart the subscriber nodes.

7. If the publisher node name was changed, restart the publisher node.

8. Sign in to the publisher CLI again and run **utils dbreplication runtimestate** on the publisher node to monitor the results of replication. We advise you to wait approximately one hour, and then verify that all nodes are in RTMT State 2.

Compressed File Name Extensions Can Cause Error Message

Normally gzip-based, compressed files have a .gz extension. Cisco Unified Presence has adopted the convention to denote open files (that is, those files currently being written to) with the special (non-standard) .gzo extension. Since these files are open, by definition the files are not terminated with the expected trailer. (That happens when the file is closed). As a consequence, some linux commands do not properly handle the gzo files or will give an error message such as:

gunzip: SDL00_00_000237.txt.gzo: unexpected end of file

You can safely ignore this message for gzo files.

Microsoft Office Communicator Remote Call Control Performance on VMWare

The performance of MOC RCC traffic on VMWare is unknown (not tested) in this release.

DRS Restore to a Smaller Virtual Machine Fails

Problem

A database restore may fail if you restore a Cisco Unified Presence server, that was originally installed on an MCS physical server, on a Virtual Machine (VM) disk.

Cause

MCS and VM disks are different in size. This condition occurs when you migrate from a larger disk size (for example, MCS with 146GB) to smaller disk size (for example, VM with 75GB).

Solution

Reconfigure the VM disk to be the same disk size or larger than the MCS server.

Known Implications for Third-Party LDAP Server Configuration when using Mozilla Firefox on a MAC Operating System

Problem

If you have a MAC operating system and use Mozilla Firefox to configure LDAP server settings in Cisco Unified Presence Administration, there is a known issue that may occur on the LDAP Server - Third-Party XMPP Clients window. Specifically, if you create a new LDAP server instance and subsequently delete the configured instance, a popup window displays and prompts you (in error) to change user passwords. This popup is not a feature of the Cisco Unified Presence Administration interface and does not display in Internet Explorer.

Cause

This condition only occurs on the LDAP Server - Third-Party XMPP Clients window in the Cisco Unified Presence Administration interface, under these specific circumstances:

1. You access the Cisco Unified Presence Administration interface using Firefox version 2.0.0.6 on a MAC operating system.

2. The Firefox browser has a saved password that is associated with the URL for accessing the Cisco Unified Presence Administration interface. To verify this on the MAC, complete these steps:

   a. Open the Firefox browser.

   b. Select **Firefox > Preferences** on the main menu.

   c. Select the Security tab.

   d. Under the Passwords section, select **Show Passwords**.

   e. When the list of sites and associated user names display, verify that the Username and Password values are associated with the URL for accessing the Cisco Unified Presence Administration interface.

3. You configure an LDAP server and subsequently delete the instance in Cisco Unified Presence Administration as follows:

   a. Select **Application > Third-Party Clients >Third-Party LDAP Servers**. Click **Add New.**

   b. Observe that the saved Username and Password values associated with the URL for accessing the Cisco Unified Presence Administration interface have been entered automatically in the Username and Password fields on this window.

   c. Enter the required information for the other fields.

   d. Enter a new Password value into the Password field. This value may or may not be different to the default value.

   e. Select **Save**. The Status message at the top of the window indicates - Add successful.

   f. Select **Delete**. A popup window displays this message: "You are about to permanently delete this LDAP Server which is required for Third-Party XMPP Client Contact Search. This action cannot be undone. Continue?"

   g. Select **Ok.** A popup window displays this message: "Please confirm which user you are changing the password for". This popup window contains the saved Username associated with the URL for accessing the Cisco Unified Presence Administration interface.

Solution

To prevent the popup window (described above) from displaying in Cisco Unified Presence Administration, you must remove the Username and Password values (associated with the URL for accessing the Cisco Unified Presence Administration interface) from the saved passwords on the Firefox browser.

Complete these steps on the MAC operating system:

1. Open the Firefox browser.

2. Select **Firefox > Preferences** on the main menu.

3. Select the Security tab.

4. Under the Passwords section, select **Show Passwords**.

5. When the list of sites and associated user names display, select **Show Password** to see the Username and Password values that are associated with the URL for accessing the Cisco Unified Presence Administration interface.

6. Locate the row that contains the following text:

    a. Site - URL for accessing the Cisco Unified Presence Administration interface

    b. Username - Value that automatically populates the Username field on the LDAP Server - Third-Party XMPP Clients window

    c. Password - Value that automatically populates the Password field on the LDAP Server - Third-Party XMPP Clients window.

    ✎

    Note It may be difficult to determine if these values match because the Password field on the LDAP Server - Third-Party XMPP Clients window is hidden from view.

7. Once you find the correct row, select it.

8. Select **Remove** to remove the saved Username and Password associated with the URL for accessing the Cisco Unified Presence Administration interface.

Results of This Procedure

- This procedure prevents the auto-population of the saved Username and Password in the Username and Password fields on the LDAP Server - Third-Party XMPP Clients window.

- It also prevent the auto-population of the saved Username and Password values in other fields associated with the Cisco Unified Presence Administration interface.

- Because the saved Username and Password values no longer exist, it prevents the popup window (described above) from displaying in error on the Cisco Unified Presence Administration interface.

Cisco Unified Personal Communicator 7.0(x) Receives a Watcher INFO Popup Until the Contact or Domain is Added to the Privacy list

Behavior

When you accept a presence request from third-party XMPP clients, the watcher is not dded to the Allow or Block list. Therefore you may experience pop-ups on Cisco Unified Personal Communicator 7.0(x) even when you have accepted or blocked the presence request on a third-party XMPP client. If the Cisco Unified Personal Communicator user is signed in to the client, the pop-up displays immediately. If the user has not signed in, the popup only displays when the user signs in.

Cause

This condition occurs because third-party XMPP clients may not modify privacy list when accepting or blocking presence requests.

Solution

The Cisco Unified Personal Communicator user continues to receive a WINFO pop-up on the client until privacy policy is applied, that is, until you add the contact or domain to the privacy list. Update the privacy list in one of these ways:

Use the..	Options:
WINFO pop-up on Cisco Unified Personal Communicator OR Privacy Preferences on Cisco Unified Personal Communicator	• Accept—Clicking Accept adds the contact to the privacy list and allows the contact to view IM and presence information. • Block—Clicking Block adds the contact to the privacy list and prevents the contact from viewing IM and presence information. • Ignore—Clicking Ignore does not modify the privacy list.
Cisco Unified Presence User Pages	1. Select **Cisco Unified Presence User pages > User Options > Privacy Policy.** 2. Select the External Users tab. 3. Add the full JID of the federated user you want to Allow or Block. Optionally you can add a federated Domain name to Allow or Block all users from this federated domain.

Federation Issues with IBM Sametime

Problem

• While XMPP subscriptions are permanent and should survive when a client signs out, IBM Sametime explicitly sends "unsubscribe" presence stanzas on signout and "subscribe presence stanzas on signin. This presents the following potential issue (observed during testing):

– If the IBM Sametime user is not in the allowed/blocked privacy list of the Cisco Unified Presence user, then the Cisco Unified Presence user always receives a popup request on MomentIM to accept the subscription whenever the federated IBM Sametime user signs in.

• IBM Sametime always sends messages to the bare JID of the Cisco Unified Presence user. This means that if the Cisco Unified Presence user is logged into multiple clients, all messages from the IBM Sametime client are always forked to each client that the Cisco Unified Presence user is signed into, regardless of which client the Cisco Unified Presence user may respond on.

• The IBM Sametime gateway has no support for composing state message stanzas (XEP-022 or XEP-085) so there is no composing state support between Cisco Unified Presence clients and federated IBM Sametime clients.

• The IBM Sametime gateway treats "unavailable" presence state as an indication the federated client is no longer available, so it does not send any further presence updates for that subscription. Subsequently, IBM Sametime will only send updates on receipt of a probe or subscribe from the federated Cisco Unified Presence user. The impact of this is observed in two places:

– Setting Manual Invisible on Cisco Unified Personal Communicator.

– Blocking an IBM Sametime user, where unavailable presence is sent to the Sametime gateway from the blocker.

- The IBM Sametime gateway does not handle XMPP message stanzas received from the PSI XMPP client correctly. Therefore, federation with IBM Sametime from PSI is not supported. If the IBM Sametime gateway receives a message stanza sent from PSI, it blocks all federated stanzas from the Cisco Unified Presence user, and a IBM Sametime gateway restart is required to recover.

Federation Group Chat Issue with GoogleTalk

It is not possible to initiate a group chat conversation with a GoogleTalk user if they are using the native GoogleTalk web or desktop clients. This issue does not occur if the GoogleTalk user were to use a third-party XMPP client.

WebEx Connect (Version 6) Client Issues

When integrating Cisco Unified Presence Release 8.0(1) with WebEx Connect (Version 6) clients, note that the following issues persist with the WebEx Connect client:

- IMs initiated from WebEx Connect clients only deliver to Cisco Unified Personal Communicator Release 7.0(x) clients that are connected to Cisco Unified Presence.

- Group chat cannot be initiated from WebEx Connect users to Cisco Unified Presence users.

It is expected that these client-side issues will be resolved in a later release of the WebEx Connect client.

Install Fails Due to Server Name Issue

Problem

The Cisco Unified Presence installation fails due to an issue with the server name.

Cause

The leading character in the server name is a digit.

Solution

None. You must change the leading character of the server name to be a letter. Cisco Unified Presence only supports server names that begin with an alphabet character.

About Cisco Unified Presence Release 8.0(2)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 8.0(2).

Client Issues when User Removes Federated Contact from their Privacy List

Problem

If a user removes a federated contact from their privacy list, it may cause unpredictable behavior to occur on the client application of the federated contact. Cisco Unified Presence terminates the federated contact's presence subscription (by sending an UNSUBSCRIBE request to the client), however, the response to the request depends on the client that the federated contact uses.

- If the federated contact uses Cisco Unified Personal Communicator 8.0(x), for example, the client removes the presence subscription to the user but the user remains in the federated contact list.

- If the federated contact uses a third-party client, such as GoogleTalk, the client sends an UNSUBSCRIBE request to Cisco Unified Presence and removes the federated contact from the contact list of the user.

The same behavior occurs if the user removes a federated domain from their privacy list. The client sends an UNSUBSCRIBE request to all federated contacts in the domain except the federated contacts that are explicitly in the privacy list.

Cause

This condition occurs as follows:

- If a user removes a federated contact from their privacy list and the federated domain is not in the privacy list

- If a user removes a federated domain from the privacy list and the federated contact is not explicitly in the privacy list

Solution

To allow Cisco Unified Presence to reestablish the presence subscription, federated contacts using Cisco Unified Personal Communicator 8.0(x) must sign out and sign back into their client application. For third-party clients, the user must add the federated contact to the contact list again.

Verifying that the Roster Migration is Complete on Cisco Unified Presence

Problem

After you perform the intercluster upgrade, the roster migration process continues on Cisco Unified Presence for the remote users for a long period and it is difficult to verify whether roster migration is complete.

Cause

This condition occurs when you perform the intercluster upgrade.

Solution

Use this procedure to verify that the roster migration is complete and the system is ready.

Note Only perform this procedure after you complete the upgrade procedure, switch Cisco Unified Presence software versions, and complete the required configuration on Cisco Unified Presence (licensing, feature configuration and start the required services). See the *Deployment Guide for Cisco Unified Presence 8.0(x)* for the intercluster upgrade procedure.

Procedure

Step 1   Run this CLI command to check the rosterupgrade queue on all nodes in the Cisco Unified Presence 8.x local cluster and all nodes in the Cisco Unified Presence 8.x remote clusters

```
run sql select count(*) from rosterupgradequeue
```

If the rosterupgradequeue table for all of the local or remote clusters is empty, the roster migration is complete. If the rosterupgradequeue table for *any* of the local or remote clusters is not empty, the roster migration is not complete yet (proceed to step 2).

Step 2   If the rosterupgradequeue is not empty and the entry on rosterupgradequeue has not decreased over time, then perform the following steps on Cisco Unified Presence:

- On the publisher node in both the local and remote Cisco Unified Presence 8.x clusters, check that the maximum contact size limitation is set to zero.

- On the publisher node in both the local and remote Cisco Unified Presence 8.x clusters, check for any system notifications.

- On the publisher node in both the local and remote Cisco Unified Presence 8.x clusters, check that the correct license file is present.

- On the publisher node, check that the required services are running, and if they are not, perform these steps:

  – Restart the Cisco UP Intercluster Sync Agent on all nodes in the Cisco Unified Presence 8.x local cluster and all nodes in the Cisco Unified Presence 8.x remote clusters.

  – On the local publisher node, restart the Cisco UP Config Agent service.

- Restart the Cisco UP XCP Router service on all local Cisco Unified Presence nodes and on all remote Cisco Unified Presence nodes.

- Restart the Cisco UP Presence Engine service on all local Cisco Unified Presence nodes and on all remote Cisco Unified Presence nodes.

- Restart the Cisco UP XCP SIP Federation Connection Manager service on all remote 7.x Cisco Unified Presence clusters.

Step 3   It may be necessary to repeat steps 1-2 until the rosterupgradequeue tables are empty on all nodes in the local Cisco Unified Presence cluster and remote Cisco Unified Presence clusters. However, note that roster migration is a CPU intensive process, and a process that takes a significant time to complete. The completion time is dependent on the size of the remote contact and rosters table in your deployment.

Troubleshooting Tips

If you switch the software version from Cisco Unified Presence Release 8.x back to Cisco Unified Presence Release 7.x on local cluster, make sure that the rosterupgradequeue table is empty on all nodes in the remote 8.x clusters before you perform an upgrade in local cluster again.

Issues for Signed In Users after Change to Proxy Domain

Problem

If you change the Proxy Domain settings on Cisco Unified Presence while users are signed into Cisco Unified Personal Communicator, all operations (including availability status and Instant Messaging (IM)) fail and users cannot sign into the updated domain.

Cause

This condition occurs if Proxy Domain settings change on Cisco Unified Presence while users are signed into Cisco Unified Personal Communicator.

Solution

Contact Cisco Support and report the credentials for the impacted user.

Non Defined Identity Management Service (IMS) Error Message Displays on Cisco Unified Presence Administration Interface

Problem

When you attempt to sign into the Cisco Unified Presence Administration interface, a "NON Defined IMS exception" error message displays.

Cause

This error message displays on the subscriber node of a two node cluster when you perform the following steps:

1. Change the LDAP credentials on Cisco Unified Communications Manager from 'SSL enabled' to 'non SSL enabled' and change the port number from 636 to 383.

2. Restart the Cisco UP XCP Router service on the subscriber node.

The error message displays because the database lookup table for the LDAP authentication returns a null value. This is due to a database replication issue on the subscriber node.

Solution

Sign into the Cisco Unified Presence Administration interface, and restart the Cisco UP Sync Agent and the Cisco UP XCP Router services.

Inability to Access Services during Upgrade

Problem

If you upgrade a cluster and the publisher node upgrades, but the subscriber node has yet to upgrade, you cannot connect to the subscriber node until its upgrade completes. An error message displays if you attempt to access the services of the subscriber node that has not yet upgraded.

Cause

This condition occurs because the subscriber node is on an older version than the publisher node.

Solution

Upgrade the subscriber node before you attempt to access services from the subscriber node on the publisher node interface.

Issue with Intercluster Deployment

Problem

You cannot add a contact in an intercluster deployment.

Cause

This condition typically occurs when the isrftrunkmeshpoint setting that controls intercluster deployment is set to false.

Solution

Run the following CLI command on the publisher node in each cluster to verify if the isrftrunkmeshpoint setting is correct:

admin:run sql select isrftrunkmeshpoint from processnode where systemnode='f'

If any value returned is 'f', run the following command to correct this:

admin:run sql update processnode set isrftrunkmeshpoint='t' where systemnode='f'

About Cisco Unified Presence Release 8.0(4)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 8.0(4).

- Unlocking a User Account on Cisco Unified Presence, page 33
- Cisco Unified Presence Release Only Supports Google Federation over TCP, page 34
- Existing Call For Microsoft Office Communicator Remote Call Control User is Placed on Hold When Second Call is Received, page 34

Unlocking a User Account on Cisco Unified Presence

Problem

If a user exceeds the permitted failed sign-in attempts or the inactivity period expires, the user account of a Cisco Unified Presence user is locked.

Cause

This condition typically occurs when the user's credential policy on Cisco Unified Communications Manager has a limit set for maximum failed logins and\or a credential expiry is set.

Solution

1. Select **Cisco Unified Communications Manager > User Management > Credential Policy.**

2. Select the appropriate credential policy relevant to the user.

3. Modify the Reset Failed Logon Attempts Every parameter value. This parameter specifies the number of minutes before the counter is reset for failed logon attempts.

4. Modify the Lockout Duration parameter value. This parameter specifies the number of minutes an account remains locked when the number of failed logon attempts exceeds the specified threshold.

5. Select **Save**.

After you perform this procedure, the user account is reset and users can sign in to Cisco Unified Presence and Cisco Unified Presence Communicator.

Cisco Unified Presence Release Only Supports Google Federation over TCP

Cisco Unified Presence supports XMPP federation with GoogleTalk over TCP. XMPP federation with GoogleTalk over TLS is not supported.

Existing Call For Microsoft Office Communicator Remote Call Control User is Placed on Hold When Second Call is Received

Problem

If a Microsoft Office Communicator Remote Call Control user takes a call on their Cisco IP phone and the user receives a second call on the same line through a blind transfer, the initial call is placed on hold automatically.

Cause

This condition typically occurs when a Microsoft Office Communicator Remote Call Control user is currently on a call and the user receives a second call on the same line through a blind transfer.

Solution

None.

Caveats

Using Bug Toolkit

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

- All severity level 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 click **Go**.

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

Open Caveats

The caveats in Table 2 describe possible unexpected behavior in the latest Cisco Unified Presence release. These caveats may also be open in previous releases. Bugs are listed in order of severity and then in alphanumeric order by bug identifier.

Table 2   Open Caveats for Cisco Unified Presence Release

Identifier	Severity	Component	Headline
CSCtf57354	3	axl	getVoicemailProfile error when voicemessagingpilot tag is included
CSCti95778	3	bat	BAT import application profiles missing audio/ccmcip profile options
CSCtj28657	3	ctigw	Existing call placed on hold when second call transferred to MOC RCC device
CSCtb98775	3	database	Slow DB response during failover causes CUPC endpoints to not login
CSCtg55258	2	database	CUPS Upgrade Failed
CSCtc87533	3	database	FreeConnectionFailover core on component shutdown
CSCti31209	3	database-ids	Jabberd core found after intercluster testing
CSCth06134	3	gui-user	CUP: Word "Users" is in English when it is translated in CUP dictionary
CSCth95227	3	intercluster	ICSA SQL error when CUCM publisher trunk not used
CSCti32971	3	intercluster	IC presence not occurring between Cisco Unified Presence Rel 8.5 and Rel 7.x clusters
CSCti75066	3	security	IPC Compliance - OpenSSL
CSCtj13037	4	security	CUP 8.0.x cup-xmpp-s2s only have CN
CSCth97812	3	sync-agent	Remove TLS entries from automatic created CTI Gateway Server

Resolved Caveats

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

Bugs are listed in order of severity and then in alphanumeric order by bug identifier. 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" section on page 34).

- Cisco Unified Presence Release 8.0(2), page 36

Cisco Unified Presence Release 8.0(2)

Table 3 lists caveats that are resolved in Cisco Unified Presence Release 8.0(2) but that may have been open in previous releases.

Table 3   Resolved Caveats for Cisco Unified Presence Release 8.0(2)

Identifier	Severity	Component	Headline
CSCte07478	3	config-agent	Moved offline IM messages not retrievable by client
CSCte43925	2	database	IDS .50.UC5X6 and X7 memory panic
CSCtd44853	3	database	CUP Tracking for CSCtc05825: ccmalarmprogram fills entire disk
CSCte57843	3	database	Database: Hostname Change Breaks Replication
CSCth38027	4	epas	Cup servername must begin with alphabet character in 7.0 or 8.0.1
CSCte98534	3	epe	XMPP Client presence not working for users with single quote in username
CSCte91081	3	epe	EPE: meeting started count and meeting ended count doesn't match
CSCtg68283	2	epe-privacy	Checking/Unchecking 'When I'm on the phone' not being set CUP side
CSCte98010	3	epe-rs	Delete roster entry when it goes from TO to NONE
CSCtg52970	3	esp	SIP Proxy: core during OPTIONs ping race condition
CSCtg71684	4	esp	User's Presence Status Not Working after Change to Proxy Domain fixed
CSCtf14376	3	gui	Persistent Chat Config Should Not Allow 'Save' w/out External DB
CSCtf31046	3	gui	XMPP LDAP service account login fails
CSCtf05385	3	gui	Third party LDAP settings vCard prompt
CSCte69546	3	gui	gui/jds: copy, add existing JDS LDAP is allowed
CSCte77781	3	gui	Presence Viewer displays incorrect warning for an invalid User ID
CSCte81095	3	gui	GUI: User IDs with "<" do not display properly.
CSCtf08915	3	gui	gui: no notification alerts when topology name changes
CSCte95285	3	gui	Cannot assume control of an Invalid Upgrade session
CSCtd74949	3	intercluster	ICSA should not synch with a 6.x cluster
CSCtf17266	3	intercluster-xml	System generated server alias not created for subscriber
CSCtb73107	3	licensing	licensing: no alarm about sw feature license
CSCtf03803	3	pws	Presence states in ref app do not map correctly
CSCtf31515	3	security	security: ldap auth fails after fresh install
CSCte93802	3	serviceability	xcp router lock on shutdown / restart
CSCte57810	3	serviceability	Wrong level for XcpDBConnectRestore
CSCte79144	3	serviceability	XCP TC counters not working in fcs throttle
CSCta75662	3	serviceability	serviceability: cli utils process delete crash doesn't gen jabber core
CSCtf05369	3	sync-agent	PE either is delayed or takes too long to be up after L2 upgrade switch
CSCte93206	3	sync-agent	In 8.x need to remove ver 5 of scripts/syncAgentSql_ver5.xml

Table 3   ***Resolved Caveats for Cisco Unified Presence Release 8.0(2) (continued)***

Identifier	Severity	Component	Headline
CSCtf05369	3	sync-agent	PE either is delayed or takes too long to be up after L2 upgrade switch
CSCtf14175	3	sync-agent	Custom LDAP Filter creation or modification requires Sync Agent restart
CSCtb83758	3	xcpauth	xcp auth debug level and indication
CSCtf09491	3	xcpauth	Need to fix static analysis issues for SXUtils.cpp
CSCtc20417	3	xcp-jds	jds: cores on ssl setup and jds start
CSCtb37115	3	xcp-jds	jds: failover not occurring
CSCtf06487	3	xcp-jsm	PCAP Sametime plugin integration issues with CUP 8.0
CSCtf08844	3	xcp-jsm	Core when a group_name of empty string exists in the groups table
CSCtd61238	3	xcp-jsm	jabberd core from pep_names_node_base
CSCte98317	3	xcp-sipgw	SIP federation Conn Mgr can exhaust allocated memory with no feedback
CSCtd44057	3	xcp-sipgw	SIP subscriptions maintained for inter-cluster after an upgrade to 8.x

Cisco Unified Presence Release 8.0(3)

Table 4 lists caveats that are resolved in Cisco Unified Presence Release 8.0(3) but that may have been open in previous releases.

Table 4   ***Resolved Caveats for Cisco Unified Presence Release 8.0(3)***

Identifier	Severity	Component	Headline
CSCth74036	1	database	L2 from 8.0.2 to 8.5.1 cause replication failures on subscribers
CSCtg70420	3	epe	Presence Exchange Gateway can't retrieve calendar for Japanese folders
CSCtg94274	2	esp	route failure stops working after 1 call, subsequent calls fail
CSCth62621	3	epe-im	SIP IM not delivered when following chars in user id: @><:/'&" space
CSCth78778	3	epe-usermove	URL Encoding wrong during user rename - requires unassign/assign
CSCth73831	3	ippm	IPPM service on CUPS fail to Response with Ack for TCP session close

Cisco Unified Presence Release 8.0(4)

Table 5 lists caveats that are resolved in Cisco Unified Presence Release 8.0(4) but that may have been open in previous releases.

Table 5   ***Resolved Caveats for Cisco Unified Presence Release 8.0(4)***

Identifier	Severity	Component	Headline
CSCti50266	2	ctigw	CTIGW: Support for Global Handle in QBE messages
CSCti71023	3	ctigw	Deskphone Placed on Autohold when New Conference is setup
CSCti45864	2	database	Invalid char in L2'd ClusterId prevents XCP Router from Starting
CSCti33125	3	database	Database out of sync between pub and sub (cucm_cdrtime records on sub)
CSCth92987	2	database-ids	Tomcat hangs waiting on DB connection
CSCth85409	2	epe	PE Does Not Start After Switch Back From 8.5 to 8.0

Table 5   Resolved Caveats for Cisco Unified Presence Release 8.0(4) (continued)

Identifier	Severity	Component	Headline
CSCtg17795	3	gui-troubleshooter	jabberd cores, out-of-memory, when troubleshooter run on large network
CSCth97726	3	soap-interface	login with any password after account lockout is permitted with CUPC7/8
CSCth20709	2	serviceability	Adding CUPS to OM goes instantly to unreachable state with SNMP timeout
CSCti85579	5	vos	vos: set password user admin warns about cucm publisher
CSCti98431	4	xcp-ma	Make startup scripts case insensitive when querying process node table

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

This section contains updates that were unavailable in the previous published versions of the following documents:

Cisco Unified Presence Release 8.0(1)

Database Setup Guide for Cisco Unified Presence

- Documentation Changes, page 39

Documentation Changes

This guide is new to Cisco Unified Presence Release 8.0. It describes how to configure an external database to store information synchronized from Cisco Unified Presence.

Instant Messaging Compliance Guide for Cisco Unified Presence

- Documentation Changes, page 39

Documentation Changes

This guide is new to Cisco Unified Presence Release 8.0. It describes how to configure the Instant Messaging Compliance feature on Cisco Unified Presence.

Hardware and Software Compatibility Information for Cisco Unified Presence

- Documentation Changes, page 40

Documentation Changes

This guide describes the hardware and software for Cisco Unified PresenceRelease 8.0(x). The compatibility information for previous releases of Cisco Unified Presence (7.0(x), 6.0(x)) are contained in separate documents on Cisco.com. For more information, see
http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

Command Line Interface (CLI) Reference Guide for Cisco Unified Presence

- Documentation Changes, page 39

Documentation Changes

This guide is new to Cisco Unified Presence Release 8.0. It lists the CLI commands for Cisco Unified Presence.

Installation and Upgrade Guide for Cisco Unified Presence

- Documentation Changes, page 39

Documentation Changes

This document extends, with this release, to provide information on the:

- bridged upgrade for customers who need to migrate from any of the discontinued hardware to supported hardware.
- installation of Cisco Unified Presence on a VMWare server.

Configuration and Maintenance Guide for Cisco Unified Presence

Documentation Changes

The Configuration and Maintenance Guide for Cisco Unified Presence has been decommissioned for this release. For Release 8.0, we integrated all of the Cisco Unified Presence administration content in a more effective online help system embedded in the Cisco Unified Presence Administration interface. The structure and contents of the online help have been enhanced (with improved parameter descriptions and examples) to better inform your decision-making as you complete tasks in the interface.

Serviceability Configuration and Maintenance Guide for Cisco Unified Presence

Documentation Changes

This updated guide contains information about the Cisco UP XCP services and new alarms that have been introduced with this release of Cisco Unified Presence.

Cisco Unified Operating System Maintenance Guide for Cisco Unified Presence

Documentation Changes

The appendix that contained the CLI commands for Cisco Unified Presence has been removed from this guide for this release, in favour of a brand new document that focuses exclusively on the CLI commands. See the *Command Line Interface (CLI) Reference Guide for Cisco Unified Presence*.

Deployment Guide for Cisco Unified Presence

Documentation Changes

The following updates are documented in the Deployment Guide for Cisco Unified Presence:

• New licensing requirements
• Updated multi-node deployment model information
• Updated multi-node installation and upgrade information
• New routing configuration information (MDNS/router to router)
• New authorization policy configuration information
• Integration of third-party XMPP clients with Cisco Unified Presence, including LDAP contact search for XMPP clients, and XMPP security mode configuration
• Configuring the Chat feature on Cisco Unified Presence, including IM gateway, chat settings, permanent chat room settings and chat room alias.

- New intercluster functionality, and performing intercluster upgrade procedures.
- Configuring an IM-only Cisco Unified Presence deployment
- Configuring multilingual support on Cisco Unified Presence

Documentation Omissions

In the *Deployment Guide for Cisco Unified Presence*, the Performing an Intercluster Upgrade procedure is missing a step between step 2 and step 3. The missing step is:

Check whether any user has reached the maximum number of contacts in the local or remote cluster. Increase the limit (if necessary).

Disaster Recovery System Guide for Cisco Unified Presence

Documentation Changes

The Restore procedure set documented in this guide is now updated to include:

- Restoring a Node or Cluster to a Last Known Good Configuration (No Rebuild)
- Restoring the First Node Only (Rebuilding the Publisher Alone)
- Restoring Subsequent Cluster Nodes (With or Without Rebuild)
- Restoring the Entire Cluster

Integration Guide for Configuring Cisco Unified Presence with Microsoft Exchange Server

Documentation Changes

The following updates are documented in the Release 8.0(x) version of this guide:

- How to Configure Multilingual Support for Calendaring Integration
- Configuring the Duration Range of Microsoft Exchange Calendar Notifications
- Uploading the Root Certificate to the Cisco Unified Presence Server - functionality changes to use the Certificate Import Tool

Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation

Documentation Changes

The following updates are documented in the Release 8.0(1) version of this guide:

- Updates to support configuring XMPP federation on Cisco Unified Presence, including configuring XMPP federation policy settings, DNS settings for XMPP federation, and configuring XMPP security certificates.
- Updates to support SIP Federation with Cisco Adaptive Security Appliance (ASA) Release 8.3.

Integration Guide for Configuring Cisco Unified Presence with Microsoft OCS for MOC Call Control

- Documentation Changes, page 42

Documentation Changes

The updated version of this guide includes updates to Line URI configuration on Microsoft Active Directory, and updates to support new certificate names on Cisco Unified Presence Release 8.0(1).

Port List for Cisco Unified Presence

- Documentation Changes, page 42

Documentation Changes

The updated version of this guide describes the port usage information for Cisco Unified Presence Release 8.0(1).

User Guide for Cisco Unified Presence

- Documentation Changes, page 42

Documentation Changes

The updated version of this guide describes new configuration for setting up user privacy policies on Cisco Unified Presence Release 8.0(1).

Cisco Unified Presence Release 8.0(2)

- Database Setup Guide for Cisco Unified Presence, page 42
- Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation, page 42
- Deployment Guide for Cisco Unified Presence, page 43

Database Setup Guide for Cisco Unified Presence

- Documentation Changes, page 42

Documentation Changes

The following updates are documented in the Release 8.0(2) version of this guide:

- Updates to support PostgreSQL, Release 8.4x
- Updates to support new hardware and performance recommendations

Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation

- Documentation Changes, page 43

Documentation Changes

The updated version of this guide supports Cisco Adaptive Security Appliance (ASA) Version 8.3(0).

Deployment Guide for Cisco Unified Presence

Documentation Changes

The updated version of this guide includes information on Cisco Unified Personal Communicator Release 8.0. It describes the following:

- Configuring basic features for Cisco Unified Personal Communicator
- Configuring voicemail, conferencing, and other features for Cisco Unified Personal Communicator
- Deploying and upgrading Cisco Unified Personal Communicator

Documentation Errors

In the Integrating the LDAP Directory chapter of the *Deployment Guide for Cisco Unified Presence*, the Fetch Contact Pictures from a Web Server topic relates only to Cisco Unified Personal Communicator Release 8.0. The correct topic title should be:

(Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server.

Also, in the Integrating the LDAP Directory chapter, the information about fetching a photo from Active Directory in the Configuring the LDAP Attribute Map for Cisco Unified Personal Communicator topic relates only to Cisco Unified Personal Communicator Release 7.1. This topic should contain the following note:

The information about fetching a photo from Active Directory in this topic relates only to Cisco Unified Personal Communicator Release 7.1.

Cisco Unified Presence Release 8.0(3)

Integration Guide for Configuring Cisco Unified Presence Release 8.0 for Interdomain Federation

Documentation Errors

Chapter: Configuring Security Certificates for XMPP Federation

    a. Section 'Importing the Self-Signed Certificate for XMPP Federation' should be titled 'Importing the Root CA Certificate for XMPP Federation'.

b. In section 'Uploading the CA-Signed Certificate for XMPP Federation', step 3 should read: Select cup-xmpp-s2s for Certificate Name.

Deployment Guide for Cisco Unified Presence

Documentation Errors

- In Chapter: Configuring the Liscencing for this Integration, in Table: Cisco Unified Presence user and server license requirements, the description for Cisco Unified Presence server liscense should read: "You can deploy Cisco Unified Presence software as a single server or as a cluster of up to three servers. You must order a separate server license for each Cisco Unified Presence server, however, you only need to upload the license to the first node in a cluster as the license file contains the number of Cisco Unified Presence servers in a cluster that are licensed to the customer."

- In chapter: Deploying and Upgrading Cisco Unified Personal Communicator, the Setting a Default Address for the Cisco Unified Presence Server topic makes several references to a CUPAddress registry subkey entry. The correct name of the registry subkey entry is CUPServer. The data type is string or REG_SZ.

- In Chapter: Configuring Basic Features for Cisco Unified Personal Communicator, the (Cisco Unified Personal Communicator Release 8.0) Configuring Settings topic, the table cell that corresponds to the CSF certificate directory (relative to CSF install directory) field should read: "This field applies only if the Client Services Framework (CSF) requires you to import security certificates to authenticate with LDAP, web conferencing, and CCMCIP. For most deployments, you do not need to import security certificates. If you must specify a value, specify the directory that contains the security certificates as an absolute path."

- In Chapter: Configuring Basic Features for Cisco Unified Personal Communicator, the Adding Users to User Groups topic states that you must add users to the Standard CTI Allow Control Of All Devices user group. This is incorrect, you do not need to add users to that user group.

- Where the Deployment Guide for Cisco Unified Presence refers to Cisco WebEx Meeting Center server, the text should be Cisco WebEx Node for MCS.

Cisco Unified Presence Release 8.0(4)

Integration Guide for Configuring Cisco Unified Presence Release 8.0 for Interdomain Federation

Documentation Changes

The overview chapter in the Integration Guide for Configuring Cisco Unified Presence Release 8.0 for Interdomain Federation should include a note that explains that Cisco Unified Presence supports XMPP federation with GoogleTalk over TCP. XMPP federation with GoogleTalk over TLS is not supported.

Obtaining Documentation and Submitting a Service Request

For information on 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.