Release Notes for Cisco Unified Presence Release 6.0(x)

Revised: May 20, 2010

These release notes describe requirements, restrictions, and caveats for Cisco Unified Presence Release 6.0(1) up to and including Cisco Unified Presence Release 6.0(7).

Note To view the release notes for previous versions of Cisco Unified Presence, choose the Cisco Unified Presence version from the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

Before you install Cisco Unified Presence, Cisco recommends that you review the "Quick Reference for URLs" section on page 2 for important documentation about Cisco Unified Presence.

Contents

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

Introduction

Cisco Unified Presence, a critical component for delivering the full value of a Cisco Unified Communications environment, collects information about user availability, such as whether users are using communications devices (for example, a phone) at a particular time. It can also collect information about individual user communications capabilities, such as whether web collaboration or video conferencing is enabled. Using this information, applications such as Cisco Unified Personal Communicator and Cisco Unified Communications Manager can improve productivity by helping employees connect with colleagues more efficiently through determining the most effective way for collaborative communication.

Quick Reference for URLs

Table 1 lists URLs for additional documentation related to Cisco Unified Presence.

Table 1 Quick Reference URLs

Related Information and Software	URL
Cisco Unified Presence Compatibility Information	http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html
Cisco Unified Presence Documentation	http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

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 Release 6.x*. Go to http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html.
  - Cisco-approved, customer-provided third-party server that is the exact equivalent of one of the supported Cisco MCS servers. Go to http://www.cisco.com/go/swonly.
- DVD-ROM drive
- Keyboard, mouse, and monitor

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.

Related Topics

- How to Upgrade Your Hardware to Cisco Unified Presence Release 6.0(6) or a Higher 6.0(x) Release from Legacy Hardware Servers, page 10

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

You can access Cisco Unified Presence Administration, Cisco Unified Serviceability, and Cisco Unified Communications OS Administration using the following browser:

  - Microsoft Internet Explorer version 6.0 or a later release

- Cisco does not support Mozilla Firefox or test with other browsers.

Installation and Upgrade Notes

- Supported Upgrade Paths to Cisco Unified Presence Release 6.0(x), page 3
- New System Installation, page 4
- Upgrade from Cisco.com, page 5
- The Latest Software Upgrades for Cisco Unified Presence on Cisco.com, page 5

Supported Upgrade Paths to Cisco Unified Presence Release 6.0(x)

Cisco Unified Presence Release 6.0(x) supports the following software upgrade paths:

- Cisco Unified Presence Release 1.0(3) to Cisco Unified Presence Release 6.0(1), 6.0(2), 6.0(3), 6.0(4) and 6.0(5).

  See the note below for information on upgrading from Release 1.0(3) to Release 6.0(6) or a higher 6.0(x) release of Cisco Unified Presence.

Caution Be aware that you cannot upgrade *directly* from Cisco Unified Presence Release 1.0(3) or earlier to Cisco Unified Presence Release 6.0(6) or a higher 6.0(x) release. This upgrade path is only permitted for hardware migration purposes. If applicable, review the information in this release note about upgrading to Cisco Unified Presence Release 6.0(6) or higher releases from legacy hardware servers.

Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 6.0(6) and Higher Releases Fail with a Sign Error

Problem

If you upgrade from Release 1.0(3) to Release 6.0(6) or higher releases of Cisco Unified Presence, the system cannot authenticate the selected signed file and the upgrade fails. Similarly, an upgrade from Release 6.0(1) to Release 6.0(6) or higher releases of Cisco Unified Presence will fail.

Cause

This condition occurs if you are upgrading from:

- current active 1.0(3) software release to 6.0(6) or higher software release.
- a current active 6.0(1) software release to 6.0(6) or higher software release.

Solution

- When upgrading from Release 1.0(3), we recommend that you upgrade to an intermediate Cisco Unified Presence 6.0(x) software release, preferably Release 6.0(5), and then upgrade that version to Release 6.0(6) or or a higher 6.0(x) release of Cisco Unified Presence.
- When upgrading from Release 6.0(1), we recommend that you upgrade to an intermediate Cisco Unified Presence 6.0(x) software release, preferably Release 6.0(5), and then upgrade that version to Release 6.0(6) or a higher 6.0(x) release of Cisco Unified Presence.

Related Topics

- How to Upgrade Your Hardware to Cisco Unified Presence Release 6.0(6) or a Higher 6.0(x) Release from Legacy Hardware Servers, page 10
- New System Installation, page 4

New System Installation

For new installations, you must order the Cisco Unified Presence system software and licensing. Go to http://www.cisco.com/en/US/ordering/ 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 6.0(1). The Cisco Unified Presence operating system and application software is installed from the installation DVD.

For new installations of the Cisco Unified Presence 6.0(x) application, use the DVD that indicates Cisco Unified Presence 6.0(x) Installation.

Related Topics

- For step-by-step installation instructions, see the *Installing Cisco Unified Presence Release 6.0(1) Guide*

Upgrade from Cisco.com

Cisco does not support downloading major Cisco Unified Presence software releases from Cisco.com, for example, Cisco Unified Presence Release 6.0(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 6.0(2) from Cisco.com.

To download this software, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml. You must have an account on Cisco.com to access the Software Center. The images posted at the Software Center require existing installations of Cisco Unified Presence.

Related Topics

- Supported Upgrade Paths to Cisco Unified Presence Release 6.0(x), page 3
- The Latest Software Upgrades for Cisco Unified Presence on Cisco.com, page 5.

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 Release 6.0(1) to 6.0(2), page 5
- Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(3), page 6
- Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(4), page 7
- Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(5), page 7
- Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(6), page 8
- Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(7), page 9

Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(1) to 6.0(2)

Before You Begin

Review the requirements for the Cisco Unified Presence 6.0(2) Engineering Special, and additional software installation instructions.

Related Topics

Cisco Unified Presence Release 6.0(2) Engineering Special, page 16

Because of its size, the original UCSInstall iso file, UCSInstall_UCOS_6.0.2.1000-27.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_6.0.2.1000-27.sgn.iso_part1of2
- UCSInstall_UCOS_6.0.2.1000-27.sgn.iso_part2of2

Procedure

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

Step 2 Execute one of the following commands to reunite the two parts of the file.

a. If you have a Unix/Linux system, cut and paste the following command from this document into the CLI to combine the two parts:

```
cat UCSInstall_UCOS_6.0.2.1000-27.sgn.iso_part1of2 UCSInstall_UCOS_6.0.2.1000-27.sgn.iso_part2of2 >
UCSInstall_UCOS_6.0.2.1000-27.sgn.iso
```

b. If you have a Windows system, cut and paste the following command from this document into the CLI to combine the two parts:

```
COPY/B UCSInstall_UCOS_6.0.2.1000-27.sgn.iso_part1of2+UCSInstall_UCOS_6.0.2.1000-27.sgn.iso_part2of2
UCSInstall_UCOS_6.0.2.1000-27.sgn.iso
```

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

- 8f76493d6697173ffe5a29b61b05c0ef UCSInstall_UCOS_6.0.2.1000-27.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_UCOS_6.0.2.1000-27.sgn.iso) to your FTP or SFTP server.
- Upgrades from Release 1.0(3) to Release 6.0(2) require the CMUpgrade_... iso file. Upgrades from Release 6.0(1) to Release 6.0(2) require the UCSInstall_... iso file

Related Topics

Image Extensions Can Cause Install Problems with Patch File Download, page 38

Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(3)

Because of its size, the original UCSInstall iso file, UCSInstall_UCOS_6.0.3.1000-12.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_6.0.3.1000-12.sgn.iso_part1of2
- UCSInstall_UCOS_6.0.3.1000-12.sgn.iso_part2of2

Procedure

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

Step 2 Execute one of the following commands to reunite the two parts of the file.

a. If you have a Unix/Linux system, cut and paste the following command from this document into the CLI to combine the two parts:

```
cat UCSInstall_UCOS_6.0.3.1000-12.sgn.iso_part1of2 UCSInstall_UCOS_6.0.3.1000-12.sgn.iso_part2of2 >
UCSInstall_UCOS_6.0.3.1000-12.sgn.iso
```

b. If you have a Windows system, cut and paste the following command from this document into the CLI to combine the two parts:

```
COPY/B UCSInstall_UCOS_6.0.3.1000-12.sgn.iso_part1of2+UCSInstall_UCOS_6.0.3.1000-12.sgn.iso_part2of2
UCSInstall_UCOS_6.0.3.1000-12.sgn.iso
```

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

- 96e714246fe65a5a7ded0244cd10d58c UCSInstall_UCOS_6.0.3.1000-12.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_UCOS_6.0.3.1000-12.sgn.iso) to your FTP or SFTP server.

Related Topics

Image Extensions Can Cause Install Problems with Patch File Download, page 38

Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(4)

Because of its size, the original UCSInstall iso file, UCSInstall_UCOS_6.0.4.1000-4.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_6.0.4.1000-4.sgn.iso_part1of2
- UCSInstall_UCOS_6.0.4.1000-4.sgn.iso_part2of2

Procedure

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

Step 2 Execute one of the following commands to reunite the two parts of the file.

a. If you have a Unix/Linux system, cut and paste the following command from this document into the CLI to combine the two parts:

```
cat UCSInstall_UCOS_6.0.4.1000-4.sgn.iso_part1of2 UCSInstall_UCOS_6.0.4.1000-4.sgn.iso_part2of2 >
UCSInstall_UCOS_6.0.4.1000-4.sgn.iso
```

b. If you have a Windows system, cut and paste the following command from this document into the CLI to combine the two parts:

```
COPY/B UCSInstall_UCOS_6.0.4.1000-4.sgn.iso_part1of2+UCSInstall_UCOS_6.0.4.1000-4.sgn.iso_part2of2
UCSInstall_UCOS_6.0.4.1000-4.sgn.iso
```

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

- 36bb921ca8210fca761a0692714be71c UCSInstall_UCOS_6.0.4.1000-4.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_UCOS_6.0.4.1000-4.sgn.iso) to your FTP or SFTP server.

Related Topics

Image Extensions Can Cause Install Problems with Patch File Download, page 38

Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(5)

Because of its size, the original UCSInstall iso file, UCSInstall_UCOS_6.0.5.1000-13.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_6.0.5.1000-13.sgn.iso_part1of2
- UCSInstall_UCOS_6.0.5.1000-13.sgn.iso_part2of2

Procedure

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

Step 2 Execute one of the following commands to reunite the two parts of the file.

a. If you have a Unix/Linux system, cut and paste the following command from this document into the CLI to combine the two parts:

```
cat UCSInstall_UCOS_6.0.5.1000-13.sgn.iso_part1of2 UCSInstall_UCOS_6.0.5.1000-13.sgn.iso_part2of2 >
UCSInstall_UCOS_6.0.5.1000-13.sgn.iso
```

b. If you have a Windows system, cut and paste the following command from this document into the CLI to combine the two parts:

```
COPY/B UCSInstall_UCOS_6.0.5.1000-13.sgn.iso_part1of2+UCSInstall_UCOS_6.0.5.1000-13.sgn.iso_part2of2
UCSInstall_UCOS_6.0.5.1000-13.sgn.iso
```

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

- 0cd698c27d712e9710db22280525b517 UCSInstall_UCOS_6.0.5.1000-13.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_UCOS_6.0.5.1000-13.sgn.iso) to your FTP or SFTP server.

Related Topics

Image Extensions Can Cause Install Problems with Patch File Download, page 38

Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(6)

Because of its size, the original UCSInstall iso file, UCSInstall_UCOS_6.0.6.1000-4.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_6.0.6.1000-4.sgn.iso_part1of2
- UCSInstall_UCOS_6.0.6.1000-4.sgn.iso_part2of2

Procedure

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

Step 2 Execute one of the following commands to reunite the two parts of the file.

a. If you have a Unix/Linux system, cut and paste the following command from this document into the CLI to combine the two parts:

```
cat UCSInstall_UCOS_6.0.6.1000-4.sgn.iso_part1of2 UCSInstall_UCOS_6.0.6.1000-4.sgn.iso_part2of2 >
UCSInstall_UCOS_6.0.6.1000-4.sgn.iso
```

b. If you have a Windows system, cut and paste the following command from this document into the CLI to combine the two parts:

```
COPY/B UCSInstall_UCOS_6.0.6.1000-4.sgn.iso_part1of2+UCSInstall_UCOS_6.0.6.1000-4.sgn.iso_part2of2
UCSInstall_UCOS_6.0.6.1000-4.sgn.iso
```

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

- 340b029b6ac22279231de6c2aec26a14 UCSInstall_UCOS_6.0.6.1000-4.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_UCOS_6.0.6.1000-4.sgn.iso to your FTP or SFTP server.

Related Topics

Image Extensions Can Cause Install Problems with Patch File Download, page 38

Accessing The Upgrade File for Cisco Unified Presence Release Release 6.0(x) to 6.0(7)

Because of its size, the original UCSInstall iso file, UCSInstall_UCOS_6.0.7.1000-5.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_6.0.7.1000-5.sgn.iso_part1of2
- UCSInstall_UCOS_6.0.7.1000-5.sgn.iso_part2of2

Procedure

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

Step 2 Execute one of the following commands to reunite the two parts of the file.

a. If you have a Unix/Linux system, cut and paste the following command from this document into the CLI to combine the two parts:

```
cat UCSInstall_UCOS_6.0.7.1000-5.sgn.iso_part1of2 UCSInstall_UCOS_6.0.7.1000-5.sgn.iso_part2of2 >
UCSInstall_UCOS_6.0.7.1000-5.sgn.iso
```

b. If you have a Windows system, cut and paste the following command from this document into the CLI to combine the two parts:

```
COPY/B UCSInstall_UCOS_6.0.7.1000-5.sgn.iso_part1of2+UCSInstall_UCOS_6.0.7.1000-5.sgn.iso_part2of2
UCSInstall_UCOS_6.0.7.1000-5.sgn.iso
```

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

- 62043875b0a08c5447da57410f49f469 UCSInstall_UCOS_6.0.7.1000-5.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_UCOS_6.0.7.1000-5.sgn.iso to your FTP or SFTP server.

Related Topics

Image Extensions Can Cause Install Problems with Patch File Download, page 38

Additional Installation and Upgrade Considerations

How to Upgrade Your Hardware to Cisco Unified Presence Release 6.0(6) or a Higher 6.0(x) Release from Legacy Hardware Servers

You cannot directly upgrade to Cisco Unified Presence Release 6.0(6) from Cisco Unified Presence Release 1.0(3). We recommend that you upgrade to an intermediate 6.0(x) release of Cisco Unified Presence (Release 6.0(5) is best), and then upgrade that version to Release 6.0(6) or or a higher release of Cisco Unified Presence. This indirect upgrade path is for hardware migration purposes only. The platform will issue alerts to this effect.

If you upgrade from an unsupported hardware server to intermediate Cisco Unified Presence Release 6.0(5) as advised above, you will need to complete the following hardware migration:

1. Upgrade the Cisco Unified Presence 1.0(3) server to Cisco Unified Presence 6.0(5). After the upgrade completes, the GUI will display the "UNSUPPORTED" warning message.
2. Back up your data on an unsupported Cisco Unified Presence 1.0(3) server.
3. Install Cisco Unified Presence Release 6.0(5) on a new hardware platform.
4. Migrate your data without changing your configuration.

In addition, you can check the Cisco Unified Presence Troubleshooter to determine if software is running on a supported hardware platform.

Prerequisites

Ensure you have the following prerequisites:

- Release 6.0(5) upgrade patch and ISO file.
- Console access to Cisco Unified Presence servers.
- Cisco Unified Presence 1.0(3) server that has already been upgraded to 6.0(5).
- New Cisco Unified Presence 6.0(5) server that meets the hardware requirement.
- Disaster Recovery System (DRS) backup server with an SFTP account.

- A license for a new hardware platform.

Note To complete hardware migration, you will need to rehost your Cisco Unified Presence license file to your new hardware. To do this, send an e-mail to licensing@cisco.com requesting a "rehost" of your license. You should include the MAC address of your current server and the new hardware platform to which you want to migrate.

Backing Up Data on an Unsupported Cisco Unified Presence1.0(3) server upgraded to 6.0(5)

Procedure

Step 1 Perform the following actions in the Cisco Unified Presence Administration login window:

a. Select **Disaster Recovery System** from the Navigation menu.

b. Click **Go**.

Step 2 Log in to the Disaster Recovery System using the same Administrator username and password that you use for Platform Administration.

Step 3

If the Disaster Recovery System is:	Action
Not already set up on your Cisco Unified Presence 1.0(3) server upgraded to 6.0(5)	**a.** Select **Backup > Backup Device**. **b.** Click **Add New** to configure a backup device in the Backup Device List window. **c.** Enter the backup device name in the Backup device name field. **d.** Select **Network Device** and enter the appropriate field values in the Select Destination area: • Server name: Name of the DRS server that stores the backup • Path name: Path name for the directory where you want to store the backup file • User name: Valid username for an account on the remote system • Password: Valid password for the account on the remote system **e.** Click **Save** to update these settings.
Already set up on your Cisco Unified Presence 1.0(3) server upgraded to 6.0(5)	**a.** Verify the following field values in the Select Destination area: • Path name: your entry must point to where the Release 6.0(5) data backup is stored **Caution** Check the **Number of backups to store on Network Directory** setting. If this field value is set to 2 and this is your third time to execute DRS to the same Path name, the first DRS will be deleted.

Step 4 Select **Backup > Manual Backup**.

Step 5 Select the backup device that you added in Step 3, in the Select Backup Device area.

Step 6 Select **CUP** and **DATABASE**, in the Select Features area.

Note If both CUPS and CUP are displayed, only select CUP.

Step 7 Click **Start Backup** to start the manual backup.

Step 8 When the backup is complete, check under the **Path name** that you have backed up files similar to the following list:

- 2007-10-03-10-47-49_drfComponent.xml
- 2007-10-03-10-47-49_esp18_cup_syslogagt.tar

- 2007-10-03-10-47-49_esp18_cup_cdpagt.tar
- 2007-10-03-10-47-49_esp18_cup_tct.tar
- 2007-10-03-10-47-49_esp18_cup_cup.tar
- 2007-10-03-10-47-49_esp18_database_db.tar
- 2007-10-03-10-47-49_esp18_cup_platform.tar
- 2007-10-03-10-47-49_esp18_database_prefs.tar

What To Do Next

Shutting Down the System, page 13

Shutting Down the System

Procedure

Step 1 Perform the following actions in the Disaster Recovery System window:

a. Select **Cisco Unified OS Administration** from the Navigation menu.

b. Click **Go**.

Step 2 Select **Settings > Version** in the Cisco Unified Communications Operating System Administration window. The Version Settings window displays and shows the software version on both the active and inactive partitions.

Step 3 Click **Shutdown** to shut down the system.

Step 4 Complete the following actions:

a. Monitor the Cisco Unified Presence server console and wait until it powers down.

b. Press the on/off switch on the Cisco Unified Presence server.

Step 5 Install Cisco Unified Presence Release 6.0(2) on a new hardware platform using the same hostname and IP.

What To Do Next

Migrating Data To a Cisco Unified Presence 6.0(5) Server Installed on New Hardware, page 13

Migrating Data To a Cisco Unified Presence 6.0(5) Server Installed on New Hardware

Procedure

Step 1 Perform the following actions in the Cisco Unified Presence Administration login window:

a. Select **Disaster Recovery System** from the Navigation menu.

b. Click **Go**.

Step 2 Log in to the Disaster Recovery System using the same Administrator username and password that you use for Platform Administration

Step 3 Select **Backup > Backup Device**.

Step 4 Click **Add New** to configure a new backup to configure a new backup device.

Step 5 Enter the backup device name in the Backup device name field.

Step 6 Click **Network Device** and enter the appropriate field values in the Select Destination area:

- Server name: Name of the DRS server that stores the backup
- Path name: Path name for the directory where you want to store the backup file
- User name: Valid username for an account on the remote system
- Password: Valid password for the account on the remote system

Step 7 Click **Save** to update these settings.

Step 8 Select **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 9 Select the backup device from which to restore in the Select Backup Device area.

Step 10 Click **Next**.

Step 11 Select the backup file that you want to restore.

Note This is the Cisco Unified Presence Release 1.0(3) data file that you backed up in the previous procedure.

Step 12 Click **Next**. The Restore Wizard Step 3 window displays.

Step 13 Select **CUP** and **DATABASE** as the features that you want to restore.

Step 14 Click **Next**.

Step 15 Click all hostnames under **Select the servers to be restored for each feature**.

Step 16 Click **Restore**.

What To Do Next

Restarting the System, page 14

Restarting the System

Procedure

Step 1 Perform the following actions in the Cisco Unified Presence Administration login window:

a. Select **Cisco Unified OS Administration** from the Navigation menu.

b. Click **Go**.

Step 2 Navigate to **Settings > Version**.

The Version Settings window displays and shows the software version on both the active and inactive partitions.

Step 3 Click **Restart**.

What To Do Next

Uploading the License File, page 15

Uploading the License File

Procedure

Step 1 After Cisco Unified Presence restarts, log in to the Cisco Unified Presence Administration using your credentials.

Step 2 Select **System > Licensing > Upload License File**.

Step 3 Click **Upload.**

Step 4 Browse to and select a license file to upload to the server.

Step 5 Click **Upload**.

Step 6 Click **Continue**.

What To Do Next

Activating Feature Services, page 15

Activating Feature Services

Procedure

Step 1 Perform the following actions:

a. Select **Cisco Unified Serviceability** from the Navigation menu.

b. Click **Go**.

Step 2 Select **Tools > Service Activation** in the Cisco Unified Serviceability window.

Step 3 Perform the following actions in the Service Activation window:

a. Select the server from the Server drop-down list box.

b. Click **Go**.

Step 4 Activate the services of the SIP Proxy and Presence Engine by checking the check box next to each one.

Step 5 Click **Save** after you finish making the appropriate changes.

What To Do Next

Verifying System Configuration, page 16

Verifying System Configuration

Procedure

Step 1 After services are activated, perform the following actions:

a. Select **Cisco Unified Presence Administration** from the Navigation menu.

b. Click **Go.**

Step 2 Select **System > Troubleshooter** and verify that the system is stable.

Cisco Unified Presence Release 6.0(2) Engineering Special

Resolved Caveats

CSCsl28100, CSCsl39615

Problem Description and Resolution

CSCsl28100 - In Cisco Unified Communications Manager 6.1, the User-Agent header format changed from "Cisco-CCMxx" to "Cisco-CUCMxx". Consequently, Cisco Unified Communications Manager 6.1 did not support the Do Not Disturb (DND) feature. The User-Agent header format is now changed to support devices in the DND state.

CSCsl39615 - If an administrator unlicensed a user in a remote cluster, the user’s contact list information was not maintained. The intercluster sync agent in Cisco Unified Presence reported zero users for unlicensed users with contacts. Cisco Unified Presence now filters users who are not licensed, and the contact list of an unlicensed user is preserved.

Special Installation Instructions

Both the Cisco Unified Presence Release 6.0(2) Installation File and the Engineering Special must be installed to address the resolved caveats. After you install the Cisco Unified Presence Release 6.0(2) Installation File, upgrade to **6.0.2.1101**.

For more information about performing a L2 upgrade, refer to the *Cisco Unified Communications Operating System Maintenance Guide for Cisco Unified Presence.*

Download File

Click here to download.

Alternatively, access the file at this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cup-ES

New and Changed Behavior

None.

Limitations and Restrictions

Table 2 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 2 Closed Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCsk40141	3	database	Cannot login to GUI Admin, CUPC Authentication fail

New and Changed Information

- Cisco Unified Presence Release 6.0(1), page 17
- Cisco Unified Presence Release 6.0(2), page 21
- Cisco Unified Presence Release 6.0(3), page 26
- Cisco Unified Presence Release 6.0(5), page 27

Cisco Unified Presence Release 6.0(1)

The following sections describe new features and changes that are pertinent to Cisco Unified Presence, Release 6.0(1) or later. The sections may include configuration tips for the administrator, information about users, and where to find more information.

- About Cisco Unified Communications Manager Alignment, page 17
- Cisco Unified Presence Features, page 18
- About Application Programming Interfaces, page 20

About Cisco Unified Communications Manager Alignment

To align with the new Cisco Unified Communications Manager 6.0(1) features, Cisco Unified Presence 6.0(1) includes the following enhancements.

- SIP Publish, page 18
- Line Appearance Based Presence, page 18
- Do Not Disturb Status, page 18
- Mobile Phone Presence, page 18

SIP Publish

For Cisco Unified Presence Release 6.0(1), Cisco Unified Communications Manager can push the presence status to Cisco Unified Presence using a PUBLISH statement, instead of Cisco Unified Presence querying for it through backend subscriptions.

In Cisco Unified Presence Administration, the Presence Gateway settings associate the presence interface with the appropriate Cisco Unified Communications Manager SIP trunk.

In Cisco Unified Communications Manager Administration, you must configure the trunk as the Cisco Unified Presence Publish trunk. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Line Appearance Based Presence

For Cisco Unified Presence Release 6.0(1), Cisco Unified Presence bases presence status on line appearances rather than on the primary extension of the Cisco Unified Presence user. You can map line appearances to users in Cisco Unified Communications Manager Administration. Associate the end user with the line appearance (**Device > Phone Configuration**). From the Phone Configuration window, click the DN that the user will use to access the Cisco Unified Presence Server. Click the Associated End Users button. From the Find and List Users window, select an end user that will access the Cisco Unified Presence.

You can also use Bulk Administration in Cisco Unified Communications Manager Administration to migrate existing users to the line-appearance-based model. Bulk Administration includes the following options:

- Export line appearances for Cisco Unified Presence users only
- Export line appearances for all the primary extensions
- Export line appearances for the devices associated

Do Not Disturb Status

Cisco Unified Communications Manager 6.0(1) includes DND Support for SIP Trunk PUBLISH. Because DND is device-based in release 6.0, if a device is changed to the DND state, all Cisco Unified Presence-enabled line appearances associated with this device could get published. When a device gets changed to the DND state, both DND as well as the busy/idle status will be published together to give Cisco Unified Presence more flexibility to process the data.

Mobile Phone Presence

Cisco Unified Presence now supports mobile presence status through Cisco Unified Communications Manager SIP PUBLISH. Presence information for mobile users can then be included in their overall reachability status. Cisco Unified Presence displays mobile phone status as a separate line appearance but will not display a separate directory number.

Cisco Unified Communications Manager only knows the status of a mobile phone that is registered within the enterprise; if the mobile is not registered, its status is published as available.

Cisco Unified Presence Features

To align with the new Cisco Unified Communications Manager 6.0(1) features, Cisco Unified Presence Release 6.0(1) includes the following features.

- What’s New Guide, page 19

- Cisco Unified Communications Manager Navigation Link, page 19
- End-User Privacy, page 19
- Calendar Integration with Microsoft Exchange, page 20
- Interclustering Support, page 20
- IP Phone Messenger Meeting Notification with Microsoft Outlook, page 20

What's New Guide

The What's New in This Release pop-up window displays the first time you start Cisco Unified Presence 6.0(1). You can also access the What's New Guide by clicking the **What's New** link on the Cisco Unified Presence Administration window or by choosing **Help > What's New**.

The What's New Guide provides the following information:

- Descriptions of new features for the current release
- Migration checklist for upgrading to Cisco Unified Presence 6.0(1)
- Links to Cisco Unified Presence technical documentation

To disable the What's New Guide pop-up window, check the **Do not display this window at startup** check box on the What's New Guide window.

Cisco Unified Communications Manager Navigation Link

For Cisco Unified Presence Release 6.0(1), the Administration main window displays a link directly to the associated Cisco Unified Communications Manager publisher server.

To open Cisco Unified Communications Manager Administration, click the **Cisco Unified Communications Manager Publisher Address** link.

End-User Privacy

To enhance privacy for the end user, Cisco Unified Presence 6.0(1) allows the user to configure customized presence rules on the User Options window. Select **User Options > Privacy > Policies**. Table 3 summarizes the available end-user privacy rules.

Table 3 End-User Privacy Rules

Rule Type	Rule Options
Visibility Rules	• Polite Blocking—Watchers always see an unavailable presence status with no device status for the user. • All state (default)—Watchers see all unfiltered device states in addition to overall reachability
Reachability Rules	• Precedence-based rules for determining reachability include Vacation, Away, Available, Busy, Unavailable. • Device type, media type, and calendar-based rules.
Filtering rules	• Exclude presence status for specific device types, media types, or calendar status.

Calendar Integration with Microsoft Exchange

The Microsoft Exchange Calendar Integration feature allows an end user to include Microsoft Outlook calendar status information in their presence status. Cisco Unified Presence updates presence status based on the status shown in Microsoft Outlook calendar, such as busy or out-of-office. End users can configure calendar integration in the User Options window.

For more information on configuring Microsoft Exchange calendar integration, see the *Cisco Unified Presence Deployment Guide*.

Interclustering Support

Cisco Unified Presence Release 6.0(1) adds support for interclustering, which enables one Cisco Unified Presence cluster to route requests to user names and phone numbers on other Cisco Unified Presence clusters. This feature enables users on different clusters to watch presence status and send instant messages to users connected to a different cluster

IP Phone Messenger Meeting Notification with Microsoft Outlook

Cisco Unified Presence Release 6.0(1) supports meeting notifications from Microsoft Exchange Server. After you configure notifications, meeting reminders not only display on the email client of the user but also will get sent to an IPPM-enabled phone, which enables the user to join a conference by simply pressing the Join key.

When a user is in a conference call, the user can also see the meeting participants on their IPPM-enabled phone. Users do not need to be active on their desktop clients to receive meeting notifications as the notifications originate from the Exchange server. Users can disable this service if the user does not want to receive meeting notifications.

About Application Programming Interfaces

To align with the new Cisco Unified Communications Manager 6.0(1) features, Cisco Unified Presence 6.0(1) includes the following programming interfaces.

- Unified Client Change Notifier (UCCN), page 20
- AXL Interface, page 20

Unified Client Change Notifier (UCCN)

Cisco Unified Presence UCCN notifies the Cisco Unified Personal Communicator of changes to the provisioning data stored in the Cisco Unified Presence database.

The UCCN detects changes within the Cisco Unified Presence database and communicates those changes to the Cisco Unified Personal Communicator using a SIP Subscribe/Notify exchange. For more information, see the *Cisco Unified Presence Interoperability Guide*.

AXL Interface

For Cisco Unified Presence Release 6.0(1), Cisco Unified Presence adds Administrative XML Layer (AXL) commands for the following functions:

- Cisco Unified Personal Communicator user configuration
- Cisco Unified Communications Manager name
- Troubleshooter

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

Cisco Unified Presence Release 6.0(2)

- Support Status for Transport Layer Security (TLS) in SIP Trunk, page 21
- How to Configure Cisco Unified Presence for Integration with Microsoft Exchange 2007, page 21

Support Status for Transport Layer Security (TLS) in SIP Trunk

TLS cannot be used to interface between Cisco Unified Presence Release 6.x and the Cisco Unified Communications Manager SIP trunk.

How to Configure Cisco Unified Presence for Integration with Microsoft Exchange 2007

Cisco Unified Presence requires an Exchange account with special permissions to query end-user calendaring data. The Exchange account must comply with the following minimum requirements:

1. Be a member of the “Exchange View-Only Administrator” group.
2. Have “Receive-As” permission on the end-user mailboxes. Cisco recommends to assign this permission at a higher level (such as mail storage group) to enable population of all the mailboxes in the mail storage group.

Note Accounts without a mailbox in the specified storage group will not work, and the account will stop working if you remove the mailbox at any stage.

Perform these procedures on the Microsoft Exchange Server to create a Receive-As account.

- Creating an Exchange Account with a Mailbox, page 21
- Delegating Roles and Receive-As Permissions to the Exchange Account, page 23
- Verifying Permissions on the Exchange Account, page 25

Creating an Exchange Account with a Mailbox

Procedure

Step 1 Log on to an Exchange 2007 server using an account that is, at least, Exchange View-Only Administrator.

Step 2 Select **Programs > Microsoft Exchange Server 2007 > Exchange Management Console** on the Windows Start menu.

Step 3 Click **Recipient Configuration** in the console tree.

Step 4 Click **New Mailbox**.

Step 5 Perform the following actions to complete the New Mailbox wizard:

Window	Configuration Steps
Introduction Window Page 1 of 6	**a.** Click **User Mailbox**. **b.** Click **Next.**
User Type Window Page 2 of 6	**a.** Click **New User**. **b.** Click **Next.**
User Information Window Page 3 of 6	**a.** Complete the required fields as described in Table 4 on page 22. **b.** Click **Next.**
Mail Settings Window Page 4 of 6	**a.** Complete the required fields as described in Table 5 on page 23. **b.** Click **Next.**
New Mail User Window Page 5 of 6	**a.** Verify your configuration, and perform one of the following actions: • Click **Back** to correct an error. • Click **Next** to proceed.
Completion Window Page 6 of 6	**a.** Click **Finish.**

What To Do Next

Delegating Roles and Receive-As Permissions to the Exchange Account, page 23.

User Information Settings

Table 4 describes the user information configuration parameters.

Table 4 User Information Configuration Parameters

Field	Description
Organizational Unit	This parameter displays the users container in Active Directory. To change the default organizational unit (OU), click **Browse** and select the OU you require.
First Name	[Optional] Enter the first name of the user.
Initials	[Optional] Enter the initials of the user.
Last Name	[Optional] Enter the last name of the user.
Name	Enter the first name, initials, and last name of the user. You can modify the name in this field.
User Logon Name (User Principal Name)	Enter the name that the user requires to log on to the mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides.
User logon Name (pre-Windows 2000)	Enter the user name for the user that is compatible with versions of Microsoft Windows that existed prior to the release of Windows 2000 Server. This field is populated by default based on the User logon name (User Principal Name) field.

Table 4 User Information Configuration Parameters

Field	Description
Password	Enter the password that the user requires to log on to his or her mailbox.
Confirm Password	Reenter the password that you entered in the Password field.
User must change password at next logon	Select this check box if you want the user to reset the password.

Mailbox Settings

Table 5 describes the mailbox configuration parameters.

Table 5 Mailbox Configuration Parameters

Field	Description
Alias	This field is automatically populated based on the User logon name (User Principal Name) of the user. You can modify the alias in this field. If any characters in the user logon name do not match the alias field, they will be replaced by underscore characters (_). The alias must not exceed 64 characters and must be unique in the forest.
Mailbox database	Click **Browse** to open the Select Mailbox Database dialog box. Select the mailbox database you require, and click **OK.** This dialog box lists all the mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. Click the title of the corresponding column to sort the databases by storage group name or server name.
Managed folder mailbox policy	Select this check box to specify a messaging records management (MRM) policy. Click **Browse** to select the MRM mailbox policy to be associated with this mailbox.
Exchange ActiveSync mailbox policy	[Optional] Select this check box to select the Exchange ActiveSync mailbox policy to be associated with this mailbox. Click **Browse**.

Delegating Roles and Receive-As Permissions to the Exchange Account

In order for Cisco Unified Presence to read Exchange calendaring data, it needs to use an Exchange account. The Exchange account must have "Receive-As" permission on all mailboxes. The Exchange account must also be an "Exchange View-Only Administrator" role."

Before You Begin

Complete the steps in Creating an Exchange Account with a Mailbox, page 21.

Procedure

Step 1 Add a user or group to an Administrator role using the Exchange Management console or Exchange Management shell.:

If you want to use the:	Action
Exchange Management Console	**a.** Log on to an Exchange 2007 server using an account that is an Exchange View-Only Administrator. **b.** Select **Programs > Microsoft Exchange Server 2007 > Exchange Management Console** on the Windows Start menu. **c.** Right-click **Organization Configuration** in the console tree. **d.** Click **Add Exchange Administrator**. **e.** Click **Browse** on the Add Exchange Administrator page. **f.** Perform the following actions in the Select User or Groups to Delegate dialog box: **g.** Select the Exchange account. **h.** Click **OK.** **i.** Select the **Exchange View-Only Administrator** role under Select the role and scope of this Exchange administrator. **j.** Click **Add**. **k.** Click **Finish** in the Completion window.

Exchange Management Shell	Run the Add-Exchange command with associated arguments from the Run line or from the Command Prompt in the Exchange Management Shell.
	The following provides the syntax and example of the command used to add a user to an administrator role:
	Syntax
	`Add-ExchangeAdministrator -Role "role" -Identity "identity"`
	Example
	`Usage: Add-ExchangeAdministrator -Role ViewOnlyAdmin -Identity CUPSAdmin`

Step 2 Run the Add-ADPermission command in the Exchange Management shell to grant Receive-As permission on the account, as follows:

Syntax

Add-ADPermission -Identity "Mailbox Store" -User "Trusted User" -ExtendedRights Receive-As

Example

Add-ADPermission -Identity "First Storage Group" -User CUPSAdmin -ExtendedRights Receive-As

Note You cannot use the Exchange Management Console for this step.

What To Do Next

Verifying Permissions on the Exchange Account, page 25.

Verifying Permissions on the Exchange Account

After you have assigned the permissions to the Exchange account, you need to verify that the permissions propagate to mailbox level, and you can access the mailbox of the end-user.

Note On Exchange 2007, it takes some time for the permissions to propagate to mailboxes.

Before You Begin

- Complete the steps in Delegating Roles and Receive-As Permissions to the Exchange Account, page 23.
- Assume, for the purpose of the examples in the following procedures, that the Exchange account is named “cupsadmin” and the mail storage group is named “First Storage Group”.

Procedure

Step 1 Access the Exchange Management shell for command line entry.

Step 2 To verify that the Exchange account is a member of “ExchangeView-Only Administrator” group, perform the following actions:

a. Run this command in the Exchange Management shell:

```
([ADSI]"LDAP://CN=CUPS Admin,CN=Users,DC=r7,DC=com").memberof
```

Note The “CN=CUPS Admin,CN=Users,DC=r7,DC=com” is the DN (Distinguished Name) of the Exchange account. You can use adsiedit.msc to determine the DN. You may also verify the DN with your Active Directory administrator.

b. Ensure that the command output indicates the Exchange account is a member of “Exchange View-Only Administrator” group, as follows:

Example: Command Output

```
CN=Exchange View-Only Administrators, OU=Microsoft Exchange Security Groups, DC=r7, DC=com
```

Step 3 To verify that the Exchange account has permissions on the mail storage group:

a. Run this command in the Exchange Management shell:

```
Get-ADPermission "First Storage Group" -user cupsadmin | Format-Table -AutoSize
```

Note The "First Storage Group" is the name of the mail storage group. The "cupsadmin" is the Exchange account.

b. Ensure that the command output indicates the Exchange account has "Receive-As" permission on the mail storage group, as follows:

Example: Command Output

```
Identity                             User           Deny         Inherited     Rights
------                               ----           ---          ------        -----
HTLUO-MAIL\First Storage Group       R7\cupsadmin   False        False         Receive-As
```

Step 4 To verify that the Exchange account has permissions on an end-user mailbox:

a. Run this command in the Exchange Management shell:

```
Get-MailboxPermission jdoe -user cupsadmin | Format-Table -autosize
```

Note The "jdoe" is the mailbox of the end user. The "cupsadmin" is the Exchange account.

b. Ensure that the command output indicates that the Exchange account has FullAccess permission on jdoe's mailbox, as follows:

Example: Command Output

```
Identity                       User           AccessRights     IsInherited      Deny
------                         ----           --------         --------         ---
r7.com/Dallas/John Doe         R7\cupsadmin   {FullAccess}     True             False
```

Note This permission is inherited from the higher-level permission, in this instance, from the "First Storage Group". If the above command returns no output, the permission has not yet propagated to the mailbox. **Do not proceed** until you see that the Exchange account has FullAccess on the mailbox of the end user.

Cisco Unified Presence Release 6.0(3)

- Recommended Best Practice for Microsoft Exchange 2007 Integration, page 26
- Exchange Calendaring Using Forms-based Authentication (FBA), page 27
- New Data Field to Authenticate Microsoft Office Communicator Users At Login, page 27

Recommended Best Practice for Microsoft Exchange 2007 Integration

Cisco recommends that the default SSL certificate, generated for Exchange on IIS, should use the Fully Qualified Domain Name (FQDN) of the Exchange server and be signed by a Certificate Authority that is trusted by Cisco Unified Presence. Configure the FQDN of the Exchange server in the:

- Exchange certificate.
- Outlook Gateway field in Cisco Unified Presence Administration.

Exchange Calendaring Using Forms-based Authentication (FBA)

Cisco Unified Presence release 6.0(3) supports the use of FBA with Microsoft Exchange 2003 and Microsoft Exchange 2007.

Related Topics

For more information on how to configure FBA for Outlook web access in Exchange 2007, see:

http://technet.microsoft.com/en-us/library/aa998867(EXCHG.80).aspx

New Data Field to Authenticate Microsoft Office Communicator Users At Login

Cisco Unified Presence allows users to log in to Microsoft Office Communicator using a new data field, that is, the value of the “msRTCSIP-primaryuseraddress” attribute from Active Directory.

Cisco Unified Presence sychronizes the data from Active Directory, and authenticates the user at login. This new data field will not effect any existing features or behavior.

As a prerequisite for this feature, ensure that Cisco Unified Presence is associated with Unified Communications Manager 6.1(3).

Cisco Unified Presence Release 6.0(5)

- Licence Change for the Cisco Phone Control and Presence with IBM Lotus Sametime Application, page 27

Licence Change for the Cisco Phone Control and Presence with IBM Lotus Sametime Application

A Cisco Unified Personal Communicator licence is no longer required to activate a user of the Cisco Phone Control and Presence with IBM Lotus Sametime application on Cisco Unified Presence. You now only need to assign one DLU, as a Cisco Unified Presence user, to activate a user of the Cisco Phone Control and Presence with IBM Lotus Sametime application.

Important Notes

- About Cisco Unified Presence Release 6.0(1), page 27
- About Cisco Unified Presence Release 6.0(2), page 30
- About Cisco Unified Presence Release 6.0(3), page 33
- About Cisco Unified Presence Release 6.0(4), page 37
- About Cisco Unified Presence Release 6.0(5), page 38
- About Cisco Unified Presence Release 6.0(6), page 41
- About Cisco Unified Presence Release 6.0(7), page 41

About Cisco Unified Presence Release 6.0(1)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 6.0(1).

IP Address Change Unsupported After Installation

Cisco recommends that you do not attempt to change the IP address of the publisher server after installing Cisco Unified Presence, either in Cisco Unified Communications Operating System Administration or by using the Command Line Interface (CLI).

If you try to do this in Cisco Unified Communications Operating System Administration, the IP configuration of the server may be lost and Cisco Unified Presence may not function properly.

The only solution, if this occurs, is to reinstall Cisco Unified Presence.

You cannot use the *set network ip* command to reconfigure the IP address and netmask via the CLI. The command does not execute successfully because of a known issue with syntax and arguments.

No Status Displays For a Buddy

Problem

If you add a user who is not known to the local Cisco Unified Presence cluster to your buddy list, no status displays for the buddy. If that user then gets licensed in a remote cluster, the user displays in the local Cisco Unified Presence cluster but the clustering code does not update the appropriate settings to cause presence to start working for the user.

Solution

After the user has been licensed on the remote server, delete the user and add it again.

Microsoft Office Communicator Logins Fail

Problem

If you run a Microsoft Live Communication Server (LCS) and the Microsoft Office Communicator (MOC) feature of Cisco Unified Presence, after Cisco Unified Presence Release 1.0(3) is upgraded to Cisco Unified Presence Release 6.0(1), MOC logins for users fail.

Cause

This condition occurs when Cisco Unified Presence Release 1.0(3) that has the CTI gateway application status set to "On" is upgraded to Cisco Unified Presence Release 6.0(1).

Solution

Disable the CTI gateway application status setting then re-enable it.

Procedure

Step 1 Log in to the Cisco Unified Presence Administration.

Step 2 Select **Application > CTI Gateway > Settings**.

Step 3 Set the Application Status setting to "Off".

Step 4 Click **Save**.

Step 5 Set the Application Status setting to “On”.

Step 6 Click **Save**.

Wait 5 minutes for data updates to complete. MOC logins should operate properly.

Cisco Unified Presence Server Upgrades

Configuration changes migrate only from older to newer versions of Cisco Unified Presence. If a Cisco Unified Presence server that has been upgraded and configured gets reverted to any previous Cisco Unified Presence release and upgraded again, any data configured in the server after the first upgrade, prior to the reversion gets erased.

Intercluster Code Cannot Determine the Correct Routing

If the same end user gets licensed for Cisco Unified Presence in two Cisco Unified Communications Manager clusters and if the two Cisco Unified Presence clusters paired with the Cisco Unified Communications Manager clusters are set up for intercluster, the intercluster code cannot determine the correct routing for the user. When the duplicate licensing is corrected, the Cisco Unified Presence clusters may not adjust appropriately.

Microsoft Office Communicator Call Forward Fails

Problem

When you use Microsoft Office Communicator to activate call forwarding on an IP phone that is logged in to extension mobility, call forwarding fails and you receive a visual indication that the operation has failed.

Cause

The Cisco Unified Communications Manager call forwarding settings get configured like this:

- The service parameter, CFA CSS Activation Policy, specifies "With Configured CSS”.
- In the Directory Number Configuration window, Forward All specifies any calling search space and the Secondary Calling Search Space for Forward All specifies none.

Solution

No workaround exists.

Server and Phone Support Information

Use this URL to find information about supported servers and phones:
http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

Cisco Unified Presence Administration GUI Drop-Down Menus Display Cryptic Values

Problem

If you change the language selection on the browser before you load a valid localization package, the Cisco Unified Presence Administration GUI displays cryptic values in the drop-down menus.

Solution

To see the valid drop-down values, select the English locale. The drop-down values display enough information to allow you to make a selection.

IPPM Automatic Meeting Reminder Feature

Problem

If you enable or disable the IPPM automatic meeting reminder feature on the **End User > Preference** menu, you should log out and then log in for the change to take effect.

Solution

In addition to the information above regarding logging out and then logging in, you can also enable or disable the meeting notification feature by using the user desk phone.

About Cisco Unified Presence Release 6.0(2)

- CTI Gateway Authentication against Cisco Unified Communications Manager is Case-Sensitive, page 30
- IBM SameTime Click-to-Call Support Information, page 31
- Allowed ACL Formats, page 31
- Exchange Server Updates, page 31
- 440 Login Timeout Errors, page 32
- Cisco Unified Presence Administration GUI Drop-Down Menus are Inaccessible, page 32
- Intercluster Code Cannot Determine the Correct Routing, page 29
- Call Forwarding Status Not Updating in Microsoft Office Communicator, page 33

CTI Gateway Authentication against Cisco Unified Communications Manager is Case-Sensitive

Problem

Application users with CTI privileges are configured with case-sensitive User IDs on Cisco Unified Communications Manager. Capital letters, lowercase letters, or a combination of both may be used. CTI Gateway application users must have identical usernames and passwords configured on both Cisco Unified Presence and Cisco Unified Communications Manager. This condition applies to all versions of Cisco Unified Presence.

Solution

When you configure CTI Gateway settings on Cisco Unified Presence, ensure that you enter the exact same application CTI Gateway username and password that you configured on Cisco Unified Communications Manager.

IBM SameTime Click-to-Call Support Information

Use this URL to find end-user support information for SameTime version 7.5, the IBM Lotus instant messaging client:

http://www-1.ibm.com/support/docview.wss?rs=477&uid=swg21195515

Allowed ACL Formats

Cisco Unified Presence accepts a range of IP address patterns in addition to a fully qualified name of an incoming host or domain. The Allow directive followed by "from" determines which hosts can access the server.

When configuring incoming and outgoing ACL settings, you can choose from the following formats:

Table 6 ACL Address Patterns

Host Address Description	Configuration Example
All hosts	• Allow from all
A partial domain name	• Allow from company.com
A full IP address	• Allow from 10.1.2.3
A partial IP address	• Allow from 10.1
A network/netmask pair	• Allow from 10.1.0.0/255.255.0.0
A network/nnn CIDR specification	• Allow from 10.1.0.0/16 **Note** The netmask consists of nnn high-order 1 bits.

Exchange Server Updates

You should ensure that your Exchange Server has the latest updates installed. Servers should be running the latest Service Packs for both Windows Server 2003 (currently SP2) and Microsoft Exchange 2003 (currently SP2).

Problem

If you encounter problems with the exchange server and it returns a "500 Internal Server Error", check that Microsoft HotFix KB841561 has been applied to your Microsoft Exchange 2003 Server.

Solution

Apply Microsoft HotFix KB841561.

Procedure

Step 1 Uninstall SP2 for Windows Server 2003 and for Microsoft Exchange 2003.

Step 2 Install SP1 for Windows Server 2003 and Exchange 2003.

Step 3 Download and install KB841561 which can be found at the following link: http://www.microsoft.com/downloads/details.aspx?familyid=050be883-11fc-4045-b988-c737e79c65d0&displaylang=en

Step 4 Install SP2 for Windows Server 2003 and for Microsoft Exchange 2003.

440 Login Timeout Errors

Problem

If the Microsoft Exchange 2003 Server has Form-Based Authentication (FBA) enabled, there is a possibility that the Exchange Server will reject calendar transactions with the error "440 Login Timeout”.

Solution

To avoid these errors, disable FBA on the Exchange server.

Cisco Unified Presence Administration GUI Drop-Down Menus are Inaccessible

Problem

If you use version 6.x of Internet Explorer to log into the Cisco Unified Presence Administration GUI, the GUI drop-down menus may be disabled after you log in.

Cause

This condition occurs when the Cisco Unified Presence server is not recognized as a trusted site.

Workaround

Add the Cisco Unified Presence server hostname to the list of trusted sites.

Procedure

Step 1 Open your IE browser.

Step 2 Select **Tools > Internet Options.**

Step 3 Select the Security tab, and click the **Trusted sites** icon.

Step 4 Click **Sites**.

Step 5 Enter the web address of the Cisco Unified Presence Administrative GUI, for example, https://<hostname>, and click **Add**.

Step 6 Click **OK.**

Intercluster Code Can Determine the Correct Routing

In Cisco Unified Presence Release 6.0(2), the intercluster code can determine the correct routing for the user even if the same end user gets licensed for Cisco Unified Presence in two Cisco Unified Communications Manager clusters, and if the two Cisco Unified Presence clusters paired with the Cisco Unified Communications Manager clusters are set up for intercluster. When the duplicate licensing is corrected, the Cisco Unified Presence clusters will automatically adjust appropriately.

Call Forwarding Status Not Updating in Microsoft Office Communicator

Problem

When you forward a call to another extension from an IP phone, the enabled Microsoft Office Communicator client for this phone may not recognize the forwarding change. In Microsoft Office Communicator, you receive a visual indication that the operation has failed with the message “Call Forwarding: OFF”.

Cause

This condition occurs when initiating Call Forwarding from an IP phone device.

Solution

To have both the Microsoft Office Communicator client and the phone recognize the forwarding change, forward the call using Microsoft Office Communicator.

Presence Update Delay on Cisco Unified Personal Communicator if the Reverse Lookup Scope is Missing

Problem

It takes approximately five seconds for presence status to update on Cisco Unified Personal Communicator.

Cause

This is due to DNS failures on the route lookup.

Solution

DNS must be configured in both directions in order to verify that the ACL is trusted. Add the reverse lookup entry for the Cisco Unified Personal Communicator subnet on the DNS server.

About Cisco Unified Presence Release 6.0(3)

Synchronizing Cisco Unified Communications Manager (Business Edition) with Cisco Unified Presence via LDAP

Problem

Cisco Unified Communications Manager (Business Edition) can be used with Cisco Unified Presence 6.x; however, Cisco Unified Communications Manager (Business Edition) 6.x does not currently support LDAP synchronization or authentication.

Cause

Cisco Unified Presence gets user information from Cisco Unified Communications Manager. The Cisco Unified Communications Manager user database can be populated one of two ways, either via manual configuration or via an LDAP synchronization. Since Cisco Unified Communications Manager (Business Edition) does not support an LDAP synchronization, the users have to be populated manually to ensure the user ID in LDAP is consistent with the configuration in Cisco Unified Communications Manager.

Solution

Users of Cisco Unified Communications Manager (Business Edition) must be configured to match the users configured in LDAP (first and last name, user ID, and directory number) and to avoid any potential mismatch of user information when using Cisco Unified Personal Communicator.

Note This limitation applies to any Cisco Unified Communications Manager that is NOT integrated with LDAP.

Switching UDP Requests to TCP

Problem

Cisco Unified Presence SIP proxy is hard-coded to use TCP for larger SIP packets (greater or equal to 1300 bytes) even if the request was intended for UDP. This also applies for Static Routes and Method/Event Routes even if UDP is configured as the specified transport in the Cisco Unified Presence Administration.

Cause:

The SIP proxy upgrades outbound UDP requests to TCP if the packet size exceeds 1300 bytes. The switch from UDP to TCP occurs, by default, if the packet size is 1300 bytes or larger. You can configure the transport type to change for any packet size between 0-65535 bytes.

Solution

This system behavior is in compliance with RFC 3261.

Sync Agent Test in System Configuration Troubleshooter

Problem

The System Troubleshooter performs a test to compare the current version of Cisco Unified Communications Manager with the version stored in the Cisco Unified Presence database, and restarts the SyncAgent if Cisco Unified Communications Manager has been upgraded. However, until the SyncAgent successfully executes at least one time, the System Troubleshooter will continue to report AXL connectivity issues with Cisco Unified Communications Manager.

Cause

This condition occurs when the SyncAgent retrieves the Cisco Unified Communications Manager version and stores it in the Cisco Unified Presence database. The Cisco Unified Communications Manager version in the Cisco Unified Presence database remains set to NULL until the SyncAgent runs successfully at least one time.

Solution

No workaround exists.

Reverse Look-up of International Dial Plans in E. 164 Format

Problem

A reverse look-up of a directory number to username will not work under these conditions:

- a Microsoft Office Communicator user is controlling the Cisco IP phone
- there is an incoming voice call to that user
- the directory number for the user is configured as E.164 in the Active Directory
- Active Directory phone number normalization rules are not set up

Under these conditions, the application identifies the call as coming from an extension number, and the username will not display in Microsoft Office Communicator.

Cause

Microsoft Office Communicator has a Reverse DN Lookup capability to:

- complete the DN- to-user id conversion
- form the proper tel url for the outbound calls

Solution

Set up the correct normalization rules for the AD address book on the Microsoft Office Communicator server, and then complete your setup and verification on the MOC client as follows:

Before you Begin

The CA-signed certificate for the OCS needs to be on the Microsoft Office Communicator PC to achieve correct certificate distribution for address book synchronization. If a common CA is used to sign certificates, for example Verisign or RSA, the CA certificate may already come installed on the PC.

Procedure

Step 1 Use this directory path to add the Normalization rules to this file:

C:\Program Files\Microsoft Office Communications Server 2007\Web Components\Address Book Files\Files\Company_Phone_Number_Normalization_Rules.txt

Tip A sample of normalization rules is provided in the Troubleshooting Tips section that follows this procedure.

Step 2 Use this directory path to run the Address Book server (ABServer) and regenerate the Normalization rules:

C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>Abserver.exe -regenUR

Note You might have to wait up to five minutes for a UR regenerate to complete successfully.

Step 3 Use this directory path to synchronize the ABServer:

C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>ABServer.exe -syncnow

Note You might have to wait up to five minutes for an ABServer synchronization to complete successfully.

Step 4 After the synchronization is complete, check the OCS server Event Viewer and verify that it indicates that the synchronization is complete.

Step 5 Test the Normalization rule on the Phone number:

C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>Abserver.exe -testPhoneNorm <E164 phone number>

What To do next

Follow this procedure to verify that the user is able to see name of the calling party in the popup window that displays when the call is made.

Complete this setup on the MOC client:

Procedure

Step 1 Exit MOC. Do not just log out.

Step 2 Delete the address book file Galcontacts.db at the following location:

C:\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\Communicator

Step 3 Start the MOC client and log in again.

Step 4 Verify that GalContacts.db is created.

Step 5 Exit MOC again, login again, and verify that the username displays in MOC.

Troubleshooting Tips

Sample Normalization rules follow:

```
# ++ test RTP
```

```
##  PSTN:+61262637900, Extension:37XXX
# +61262637ddd
[\s()\-\./\+]*(61)?[\s()\-\./]*0?(2)\)?[\s()\-\./]*(6263)[\s()\-\./]*(7\d\d\d)
3$4;phone-context=dialstring
# ++ test1 RTP
## Site:, PSTN:+61388043300, Extension:33XXX
[\s()\-\./\+]*(61)?[\s()\-\./]*0?(3)\)?[\s()\-\./]*(8804)[\s()\-\./]*(3\d\d\d)
3$4;phone-context=dialstring
#Test input +61388043187, Test result-> tel:33187;phone-context=dialstring
# ++ test2 RTP
##  PSTN:+61292929000, Extension:29XXX
[\s()\-\./\+]*(61)?[\s()\-\./]*0?(2)\)?[\s()\-\./]*(9292)[\s()\-\./]*(9\d\d\d)
2$4;phone-context=dialstring
# Test input +61292929761, test result-> tel:29761;phone-context=dialstring
```

Duplicate Users in Cisco Unified Presence Limited to 250 Records

Problem

In Cisco Unified Presence, the Duplicate User List only displays the first 250 records.

Cause

Configure an intercluster Cisco Unified Presence environment that contains more than 250 duplicate users licensed to multiple Cisco Unified Presence servers.

a. Select **System > System Status.**

b. Click the duplicate user hyperlink.

Only the first 250 duplicate users are displayed. The UI does not display User 251 and higher.

Solution

Using the Platform CLI on Cisco Unified Presence, run the following command:

run sql select unique c.userid, c.peerid pub from cupsuserlocation c, cupsuserlocation d where c.userid=d.userid and d.peerid!=c.peerid

This command reports the duplicate user and the publisher of the cluster to which the user has been licensed. If the value of "local" returns for the publisher, that user is licensed on the local Cisco Unified Presence cluster associated with the SQL query.

About Cisco Unified Presence Release 6.0(4)

- Call Transfer Fails Via SIP Proxy, page 37
- Release 6.0(3) to 6.0(4) Upgrade of Cisco Unified Presence Does Not Preserve CA Certificate, page 38

Call Transfer Fails Via SIP Proxy

Problem

When a call is transferred, the SIP Proxy routes a mid-call Invite message. The Request URI incorrectly updates to match the next hop address and does not maintain the contact address of the endpoint. As multiple hops are traversed, the call transfer fails after 30 seconds.

Cause

This condition occurs when a call is a transfer call. The issue could also occur on a direct call, when a re-invite message updates the session timer.

Solution

No workaround exists.

Release 6.0(3) to 6.0(4) Upgrade of Cisco Unified Presence Does Not Preserve CA Certificate

Problem

Integration betweenCisco Unified Presence and the Microsoft Exchange server does not work after you upgrade from Cisco Unified Presence Release 6.0(3) to 6.0(4).

Cause

This condition occurs because the CA certificate that was uploaded via the backend Presence Gateway window is not preserverd during an upgrade of Cisco Unified Presence from Release 6.0(3) to 6.0(4).

Solution

Re-upload the CA certificate without the subject Common Name (CN) in the backend Presence Gateway page. This ensures that the Exchange certificate will be signed.

About Cisco Unified Presence Release 6.0(5)

Image Extensions Can Cause Install Problems with Patch File Download

Problem

When the Cisco Unified Presence upgrade patch file is downloaded from cisco.com, some browsers may download files with the extension tar.gz.sgn as tar.gz.gz. The .gz.gz file cannot be successfully installed.

Cause

This condition occurs if you use Internet Explorer or Opera browsers to download the signed Cisco Unified Presence patch file from cisco.com.

Solution

After the patch file is downloaded, rename it with the extension .gz.sgn (in place of.gz.gz) and proceed with the install. Alternatively, use a Mozilla-based browser such as Firefox (any version) to download the patch file.

AXL executeSQLQuery Request Hangs or Fails on Large Request

Problem

If an AXL executeSQLQuery is sent that returns a large data set (greater then 16 MB), it can cause the Tomcat web server to hang or to reject the request.

Cause

This condition occurs when an AXL executeSQLQuery is sent that returns a data set that contains a large number of rows in a database table.

Solution

Retrieve the data in chunks using the format "select skip X first Y * from table".

Cisco Unified Presence Engine Database Service is not Correct in SYSAPPL-MIB

Problem

No valid SNMP management information is available for the Cisco Unified Presence Engine Database service beyond the basic sysApplInstallPkgProductName.

Cause

This condition occurs in a basic Cisco Unified Presence configuration with SNMP enabled.

Solution

No workaround exists.

Sync Agent Fails to Synchronize Data from Cisco Unified Communications Manager

Problem

If large queries are being sent to Cisco Unified Communications Manager via AXL, the Cisco Unified Presence Sync Agent can fail to synchronize data from Cisco Unified Communications Manager. In some cases the AXL request from the Sync Agent will hang and in others it will receive this error: "Maximum AXL Memory Allocation Consumed".

Cause

This condition occurs when the Sync Agent synchronizes data from Cisco Unified Communications Manager while large AXL queries are being sent to Cisco Unified Communications Manager.

Solution

Restart the Sync Agent.

Config Agent Static routes Do Not Update Correctly

Problem

Static routes send messages to a wrong (previously entered) address.

Cause

If a customer changes a static route, while the config-agent is down, the route will be updated in the database but not on the server. The server will continue to use the previous setting.

Solution

First enable Routing debugs and examine the logs. If routing to the address does not match the current configuration, you must:

- add the original route again,
- then delete the route again,
- and add the route once more to a new destination.

IPPM : XML Parse Error when showing Message History

Problem

After receiving a message in Japanese, an XML Parse Error may occur when showing the Message History (IPPM Service -> Messages).

Cause

This problem may occur for languages other than English, in this setup environment:

- Cisco Unified Communications Manager—6.1.2.1000-13
- IP Phone 7975—8.3.4SR1, 8.3.5
- Cisco Unified Presence— 6.0.4.1000-4

Solution

No workaround exists.

MOC Call Transfers to External Destinations Fail

Problem

The CTI call transfer request that Cisco Unified Presence uses to relay from MOC to Cisco Unified Communications Manager is empty. As a result, the call transfer via MOC fails.

Cause

This occurs in the following conditions:

- External party A with CSS calls party B (MOC).
- Party B then transfers the call to an external party C.
- Currently the CTIGW instructs Cisco Unified Communication Manager to use the CSS of party A to transfer the call to party C. Because there is no such a dial plan, the transfer fails.

Solution

No workaround exists.

Disabling DNS and Reverse DNS Lookup on Cisco Unified Presence for CVP integration

Problem

Reverse DNS lookup queries on Cisco Unified Presence may take longer to process if there are network issues or problems with the DNS server. Delays can occur if you do not use DNS, or IP addresses, in your Cisco Unified Presence and CVP environment.

Cause

The delay occurs because Cisco Unified Presence continues to wait for a response from the DNS server.

Solution

If you are not using DNS in your network configuration, do not adda DNS entry on Cisco Unified Presence. Perform the following actions to disable Reverse DNS lookup:

- Run **delete dns <ipaddress>** from the CLI.
- Set the "A-record IP lookup" service parameter to OFF.
- Reboot the Cisco Unified Presence server.

About Cisco Unified Presence Release 6.0(6)

- Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 6.0(6) Fail with a Sign Error, page 41

Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 6.0(6) Fail with a Sign Error

For more information, see Supported Upgrade Paths to Cisco Unified Presence Release 6.0(x), page 3.

About Cisco Unified Presence Release 6.0(7)

- Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 6.0(7) Fail with a Sign Error, page 41

Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 6.0(7) Fail with a Sign Error

For more information, see Supported Upgrade Paths to Cisco Unified Presence Release 6.0(x), page 3.

Caveats

- Using Bug Toolkit, page 42
- Open Caveats, page 42
- Resolved Caveats, page 42

Using Bug Toolkit

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

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

You can search for problems by using the Cisco Software Bug Toolkit.

Before You Begin

- To access Bug Toolkit, you need the following items:
  - Internet connection
  - Web browser
  - Cisco.com user ID and password

Procedure

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

Step 2 Log 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.

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

Open Caveats

The caveats in Table 7 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 7 Open Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCsi10758	3	ctigw	In a scenario where a Microsoft Office Client (MOC) is used to control an IP Phone, the activation/deactivation of Call Forwarding using the IP Phone does not get updated on the MOC GUI

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 42).

Cisco Unified Presence Release 6.0(2)

Table 8 lists caveats that are resolved in Cisco Unified Presence Release 6.0(2) but that may have been open in previous releases.

Table 8 Resolved Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCsj25632	2	ctigw	The SIPD process randomly crashes when customer runs Microsoft Office Communicator traffic
CSCsj25666	2	ctigw	MOC Call Forward Fails
CSCsi29201	3	ctigw	MOC Unannounced Transfer to Busy Dest Fails Without Indication
CSCsj20205	2	database	MOC log in fail
CSCsj27926	2	database	Fix Side Effect of Slow MOC Login Fix For Cluster - Replication Issue
CSCsj40135	3	database	Remove internal AXL API from WSDL
CSCsj45575	3	database	IPPM lookup of alias by extension returns same userid multiple times
CSCsj33794	3	epe	No notify record exists to generate notify
CSCsi33773	6	epe	In CUP, Exchange Calendar integration always expects a users calendar to be stored under the folder name "calendar". In international versions of Microsoft Exchange, the information may be stored under a different localized name
CSCsj36718	3	esp	Seeing CANCEL to INVITE sent and no response
CSCsi02258	3	gui	Input in the ServerName field needs validation check
CSCsj17136	3	gui	The Cisco Unified Presence troubleshooter indicates that the SyncAgent needs to be restarted
CSCsj44432	3	gui	TLS Subject Peer configuration window rejects subject names that contain spaces
CSCsj27604	3	gui	Meeting Notification turned off on preference page save
CSCSi18682	2	intercluster	Two CUP clusters that contain duplicate userids cause invalid routing of presence status. **Note:** This defect has been superseded by CSCsj15342
CSCsj15342	2	intercluster	Intercluster sync agent doesn't update entry when duplicate removed
CSCsj42040	3	oamagent	Messages sent between the SIP Proxy and presence engine on the same server use TCP as the transport type

CSCsj35060	2	sync agent	ICSync-Agent audit causes traffic backup that leads to memory errors
CSCsh73262	3	sync agent	SyncAgent mistakenly deletes roles/groups
CSCsj34597	1	vos	One server experiences a reboot hang issue that is specific to the platform code in Cisco Unified Communications Manager. This server is on New Product Hold.
CSCsj10960	2	vos	cmahealthd process might dump core when system is under high-load stress
CSCsi65560	2	vos	Soft interrupt CPU is high

Cisco Unified Presence Release 6.0(3)

Table 9 lists caveats that are resolved in Cisco Unified Presence Release 6.0(3) but that may have been open in previous releases.

Table 9 Resolved Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCsk48337	2	ctigw	Microsoft Office Client (MOC) end-to-end calls not completing when using TLS connections between CUP and Office Communications Server (OCS).
CSCsk67670	3	database	CUPS single-node enabled for replication causes DDRBlock
CSCsi98679	3	database	Active Directory LDAP attribute mappings incorrect.
CSCsh97277	3	database	Presence events exist for deleted contacts.
CSCsi89532	3	GUI	Second node proxy ACL configuration window displays error.
CSCsk81391	3	GUI	User page: Java error
CSCsk80676	3	GUI	Incorporate GUI Notification for Unsupported CCM Releases
CSCsi13752	3	GUI	When Internet Explorer refreshes an Cisco Unified Presence Administration window, only the Save icon displays.
CSCsi17814	3	GUI	Presence and instant messaging to and from a peer that resides in a foreign domain does not work. The Cisco Unified Presence proxy server returns 4xx responses to requests sent to the remote server.
CSCsi52062	3	GUI	Troubleshooter returns internal error in report.
CSCsj09239	3	GUI	User cannot change user preferences when there is no outlook gateway
CSCsj27401	3	GUI	Use SSL should not enforce the use of port 443r.
CSCsh84741	6	GUI	In the Cisco Unified Presence User Options application, contacts that get hosted on a non-local server will not display their login status.
CSCsj26573	3	IPPM	No call back or join sofIPPMtkeys exist in a MeetingPlace meeting.
CSCsk93310	3	SOAP Interface	AXL doesn't handle userid with a quote in it
CSCsi88233	4	sync agent	No available connections message occurs hourly.
CSCsk45151	3	vos	SA and ICSA log timestamps are behind by 1hr when NZ DST changes.

Cisco Unified Presence Release 6.0(4)

Table 10 lists caveats that are resolved in Cisco Unified Presence Release 6.0(4) but that may have been open in previous releases.

Table 10 Resolved Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCsq77790	2	ctigw	MOC c2call delay in call disconnect and popup for incoming calls
CSCsr04868	3	database	MOC login fails due to spValDevice
CSCsq66270	3	esp	CUPS 6.0.2-1000-27-Core Dumps **Note** This defect is not resolved in the 6.0(4) Cisco Unified Presence base; it is only resolved in the Engineering Special release of Cisco Unified Presence 6.0.4.

Cisco Unified Presence Release 6.0(5)

Table 11 lists caveats that are resolved in Cisco Unified Presence Release 6.0(5) but that may have been open in previous releases.

Table 11 Resolved Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCso07061	1	esp	CUPS generates core dumps under load with CVP 7.0.1
CSCsw14321	3	ctigw	CCM Cti Failover/Fail Back Back Does Not Seem To Work with RCC Control
CSCsv78069	3	ctigw	MOC not open window for incoming call when Auto Call Pickup is Enabled
CSCsu54916	3	database	DB: No presence for buddy added via CUPC but OK when added via GUI
CSCsi27935	3	vos	Netdump client start failed on subscribe node
CSCsm97683	3	epe	PE core dumped when CUCM gateway was configured after I started services
CSCsv52431	3	esp	esp: improper handling of branches after timeout
CSCsl04891	3	ippm	IPPM XML Parse error on Deskphone if already logged into IPPM on 7921
CSCsv79153	3	ippm	IPPM:XML Parse Error when showing Message history
CSCsr90338	3	ippm	IPPM didn't show 'Dial' softkey upon receiving IM
CSCsr48752	3	security	CUPS upgrade didn't carry PE-trust certs over in Tomcat directory
CSCso29090	3	serviceability	Improve error message when failing to activate services
CSCsr28889	3	sync agent	By updating an AD user, the user fails to log in CUPC and CUP User page
CSCsv14860	3	sync agent	SA Change Notification SQL Exception(inserting): Error Code: -691
CSCsv05264	3	vos	Proxy: empty response code during timeout
CSCsr04868	3	database	MOC login fails due to spValDevice

Cisco Unified Presence Release 6.0(6)

Table 12 lists caveats that are resolved in Cisco Unified Presence Release 6.0(6) but that may have been open in previous releases.

Table 12 Resolved Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCtf25408	4	vos	Port CSCsr74305 ntp_one_shot.sh intermittently kills wrong processes

Cisco Unified Presence Release 6.0(7)

Table 13 lists caveats that are resolved in Cisco Unified Presence Release 6.0(7) but that may have been open in previous releases.

Table 13 Resolved Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCsm90310	3	cpi-os	snmpd has memory leak on HP servers (RHEL 3 CUCM's only)
CSCtf17294	3	ccmbuilds	/vob/ccm_buildtools/build path needs to be added to the 6.x environment
CSCtf81211	2	gui	Remove trademark infringement

Documentation Updates

- Cisco Unified Presence Release 6.0(1), page 46
- Cisco Unified Presence Release 6.0(2), page 47
- Cisco Unified Presence Release 6.0(3), page 59

Cisco Unified Presence Release 6.0(1)

This section provides documentation changes that were unavailable when the Cisco Unified Presence Release 6.0(1) documentation suite was released.

- Omissions, page 46
- Errors, page 47

Omissions

This section contains information that may have been left out of the documentation for Cisco Unified Presence Release 6.0(1).

Intercluster Peers

The following two parameters apply to the Intercluster Peers chapter of the *Cisco Unified Presence Administration Guide*:

- Protocol: This parameter specifies the preferred protocol type used by the intercluster sync agent when determining the protocol for Cisco Unified Presence intercluster SIP traffic. If the specific protocol is configured in the remote Cisco Unified Presence cluster, then “Protocol” is used. If the remote cluster does not contain a Cisco UP SIP Proxy listener of “Protocol” type, then a protocol is selected according to the following precedence: UDP, TCP, TLS.

- External Phone Number Mask: This parameter specifies the default E164 external phone number mask to associate with each DN that synchronizes from the remote Cisco Unified Communications Manager / Cisco Unified Presence cluster. The default E164 mask is overridden by the E164 mask assigned to a Line Appearance from the remote cluster. IP Phone Messenger uses the DN and E164 mask from the remote cluster for dial back functionality.

Errors

This section contains information about inaccuracies in the documentation for Cisco Unified Presence Release 6.0(1).

IP Phone Messenger Settings

The IP Phone Messenger Settings chapter in the *Cisco Unified Presence Administration Guide* incorrectly lists the following two parameters, which are not available in Cisco Unified Presence 6.0(1):

- SIP Subscribe Event Package
- SIP Subscribe Event Header

Cisco Unified Presence Release 6.0(2)

This section provides documentation changes that were unavailable when the Cisco Unified Presence Release 6.0(1) documentation suite was released.

- Omissions, page 47
- Errors, page 58

Omissions

This section contains information that may have been left out of the documentation for Cisco Unified Presence Release 6.0(1).

Proxy Static Routes Precedence

The following example should be added to the Static Routes chapter of the *Cisco Unified Presence Administration Guide* to clarify how the priority and weight associated with a route determines precedence.

Consider these three routes with associated priorities and weights:

- 1, 20
- 1, 10
- 2, 50

In this example, the static routes are listed in the correct order. The priority route is based on the lowest value priority, that is 1. Given that two routes share the same priority, the weight parameter with the highest value decides the priority route.

Required User permissions for Intercluster Peer Configuration

Problem

Permissions required for the Cisco Unified Presence intercluster peer user are not documented in the Intercluster Peers chapter of the *Cisco Unified Presence Administration Guide*.

Solution

The administrator can grant allowed permissions based on user roles. If necessary, add SuperUser permissions to the user assigned as the Cisco Unified Presence intercluster peer in Cisco Unified Communications Manager.

Configuration Troubleshooter: Interclustering Test

The following Intercluster test applies to the Configuration Troubleshooter chapter of the *Cisco Unified Presence Administration Guide*:

Problem

One or more users are licensed in more than one Cisco Unified Presence cluster. This causes inconsistent presence and instant message routing.

Solution

Determine the true cluster to which each of the duplicate users belongs. Investigate which of the Cisco Unified Communications Manager clusters associated with the Cisco Unified Presence cluster has the user incorrectly licensed for Cisco Unified Presence.

Intercluster Peer Duplicates Navigation Link

There is an additional hyperlink description that should be added to the Status chapter of the *Cisco Unified Presence Administration Guide.* The Cisco Unified Presence System Status window displays a link when end users associated with an intercluster peer are duplicated.

To view the duplicate users, click the **X Duplicates found** link.

Uploading Microsoft Exchange Certificates

The following should be added to the "Exchange Calendar Integration Configuration" section of the *Cisco Unified Presence Deployment Guide*.

Cisco Unified Presence Release 6.0(2) allows you to upload Exchange server trust certificates with or without a Subject Common Name (CN).

- If a certificate has a Subject CN, upload the certificate through the Cisco Unified OS Administration GUI. Select **Security > Certificate Management.**
- If the certificate has no Subject CN, upload the certificate on the Presence Gateway Configuration page of the Cisco Unified Presence Administration GUI. Select **Cisco Unified Presence > Presence Engine > Presence Gateways.** You can upload any number of root CA certificates but you must upload five certificates at a time. Following a L2 upgrade, the Exchange certificates must be uploaded again on this page.
- For a third-party CA- signed Exchange server certificate, you must upload all CA certificates in the certificate chain to Cisco Unified Presence as a Presence Engine (PE) trust certificate.

Note Restart the Presence Engine and SIP Proxy after you upload all Exchange trust certificates. This requirement applies to both upload methods if the Meeting Notification feature is used. After a certificate is uploaded, the Presence Engine must be restarted first followed by the Proxy restart. You can upload all certificates and then start these services.

Uploading CA-Signed Certificates

The following step should be added to the "Configure the Security Certificate" section of the *Cisco Unified Presence Deployment Guide*. To complete the certificate exchange process, the user must upload the signed certificate to the Cisco Unified Presence server after uploading it to the CA server.

When you upload a signed certificate to Cisco Unified Presence, you must state the root certificate name by specifying the.PEM filename as it appears in the certificate list.

Procedure

Step 1 Select **Security> Certificate Management**.

Step 2 Click **Find** in the Certificate List window**.**

Step 3 Locate the root certificate that has signed the certificate you want to upload.

Note The root certificate should appear in this list alongside its .PEM filename. If the root certificate's original filename did not match its Subject Common Name when it was uploaded, the .PEM filename will be different. Use the Subject CN and the trust-store service (for example, sipproxy-trust) to find the certificate in the list.

Step 4 Perform the following actions:

a. Highlight the certificate's .PEM file name with the cursor.

b. Select **Edit > Copy** from the web browser menu.

Step 5 Click **Upload Certificate**.

Step 6 From the Certificate Name list, select the appropriate certificate name.

Step 7 Select **Edit > Paste** [CTRL+V] to paste the .PEM filename of the CA certificate in the Root Certificate text box.

Step 8 Select the file to upload by completing one of the following steps:

a. Enter the path to the file in the Upload File text box.

b. Click **Browse** and navigate to the file; then, click Open

Step 9 Click **Upload File** to upload the certificate to the Cisco Unified Presence server,

How to Configure the LCS Certificate Chain

The LCS certificate configuration process should be added to the Microsoft Integration Overview chapter of the *Cisco Unified Presence Deployment Guide.*

To configure an LCS certificate on the LCS server, complete the following tasks:

- Downloading the CA certification chain.
- Installing the CA certification chain.
- Requesting the Certificate.
- Manually approving a certificate issuance request after the request is made.

Downloading a CA Certification Chain

Procedure

Step 1 Perform the following actions:

a. Click **Start > Run**

b. Type **http://<name of your Issuing CA Server>/certsrv**.

c. Click **OK**.

Step 2 From Select a task, click **Download a CA certificate, certificate chain, or CRL**.

Step 3 From Download a CA Certificate, Certificate Chain, or CRL, click **Download CA certificate chain**.

Step 4 Click **Save**.

Troubleshooting Tips

Step 5 Save the file on a hard disk drive on your server. This file has an extension of .p7b. If you open this .p7b file, the chain will have the following two certificates:

- name of Standalone root CA> certificate
- name of Standalone subordinate CA> certificate(if any)

Installing a CA Certification Chain

Procedure

Step 1 Perform the following actions:

a. Click **Start > Run**

b. Type **mmc**.

c. Click **OK**.

Step 2 Select **Add/Remove Snap-in** from the File menu.

Step 3 Click **Add** in the Add/Remove Snap-in dialog box.

Step 4 Select **Certificates** in the list of Available Standalone Snap-ins.

Step 5 Click **Add**.

Step 6 Select Computer account and click **Next**.

Step 7 In the Select Computer dialog box, complete the following tasks:

a. Ensure **Local computer: (the computer this console is running on)** is selected.

b. Click **Finish**.

Step 8 Click **Close.**

Step 9 Click **OK**.

Step 10 In the left pane of the Certificates console, expand Certificates (Local Computer).

Step 11 Expand Trusted Root Certification Authorities.

Step 12 Perform the following actions:

a. Right-click **Certificates.**

b. Point to All Tasks.

c. Click **Import**.

Step 13 Click **Next** in the Import Wizard.

Step 14 Complete the following tasks:

a. Click **Browse** and go to where you saved the certificate chain.

b. Select the p7b file.

c. Click **Open**.

Step 15 Click **Next**.

Step 16 Leave the default value **Place all certificates in the following store** and ensure **Trusted Root Certification Authorities** appears under the Certificate store.

Step 17 Click **Next**.

Step 18 Click **Finish.**

Requesting a Certificate

Procedure

Step 1 Perform the following actions on the computer requiring a certificate:

a. Open a Web browser and type the URL **http://<name of your Issuing CA server>/certsrv.**

b. Press **Enter**.

Step 2 Click **Request a Certificate**.

Step 3 Click **Advanced certificate request**.

Step 4 Click **Create and submit a request to this CA**.

Step 5 Click **Other** in the Type of Certificate Needed list.

Step 6 In the Name field of the Identifying Information section, type the **<FQDN> (fully qualified domain name**.

Note The name must match the name of the LCS, which is usually the FQDN.

Step 7 In the OID field, type the following OID: **1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2**.

Note A comma separates the two 1s in the middle of the OID.

Step 8 In Key Options, check **Store certificate in the local computer certificate store**.

Step 9 Enter a friendly name.

Step 10 Click **Submit**.

Step 11 Click **Yes** in the Potential Scripting Violation dialog box

Manually Approving a Certificate Issuance Request

Procedure

Step 1 Log on to the enterprise subordinate CA server with Domain Administrator credentials.

Step 2 Perform the following actions:

a. Click **Start > Run.**

b. Type **mmc**.

c. Press **Enter.**

Step 3 Select **Add / Remove Snap-in** from the File menu.

Step 4 Click **Add**.

Step 5 In Add Standalone Snap-in, complete the following tasks:

a. Click **Certification Authority.**

b. Click **Add**.

Step 6 In Certification Authority, accept the default option, **Local computer (the computer this console is running on**).

Step 7 Click **Finish**.

Step 8 Click **Close.**

Step 9 Click **OK.**

Step 10 In the MMC, expand Certification Authority and expand your issuing certificate server.

Step 11 Click **Pending request**.

Step 12 In the Details pane, perform the following actions:

a. Right-click the request identified by its request ID.

b. Point to All Tasks.

c. Click **Issue**.

Step 13 Click **Start > Run** on the server from which you requested the certificate.

Step 14 Type **http://<name of your Issuing CA Server>/certsrv** and click **OK**.

Step 15 From Select a task, click **View the status of a pending certificate request**.

Step 16 From **View the Status of a Pending Certificate Request,** click your request.

Step 17 Click **Install this certificate**.

Step 18 Complete the following actions on the LCS Admin Page:

a. Right-click on the desired server.

b. Select **Properties.**

Step 19 From the Security tab, complete the following tasks:

a. Click **Select Certificate.**

b. Select the newly installed LCS certificate.

Uploading Supported x509 Certificates

The following x509 formats for user-uploaded certificates should be added to the Security chapter of the *Cisco Unified Communications Operating System Administration Guide*.

SIP Proxy and Presence Engine certificates (own and trust) should be X.509 version 3 compliant. Tomcat certificates (own and trust) should be X.509 version 1 compliant.

Enabling and Disabling Empty TLS Fragments

There is an additional checkbox description that should be added to the TLS Context Configuration chapter of the *Cisco Unified Presence Administration Guide.* The TLS Configuration window displays a checkbox that allows users to enable or disable empty TLS fragments.

The checkbox is checked by default.

Managing Live Communications Server (LCS) Security Certificates

The certificate exchange process between Cisco Unified Presence and LCS should be added to the Cisco Unified Presence Configuration Overview chapter of the *Cisco Unified Presence Deployment Guide*.

	Task	Procedure
Step 1	Download the root certificate	**a.** Log in to your CA server and open a web browser. **b.** Open the following URL: – http://127.0.0.1/certsrv **c.** Click **Download a CA certificate, certificate chain, or CRL**. **d.** For the Encoding Method, select **Base 64**. **e.** Click **Download CA Certificate**. **f.** Save the certificate, **certnew.cer**, to the local disk. **Note** If you do not know the Subject Common Name (CN) of the root certificate, you can use an external certificate management tool to find out. On Windows operating system, you can right-click the certificate file with a .CER extension and open the certificate properties.
Step 2	Upload the root certificate into the trust store of the Cisco Unified Presence server.	**a.** Copy or FTP the certnew.cer certificate file to the computer that you use to administer your Cisco Unified Presence server. **b.** From the Navigation menu on the Cisco Unified Presence Administration login window, complete the following actions: • Select **Cisco Unified OS Administration**. • Click **Go**. **c.** Enter your username and password for Cisco Unified Operating System Administration and click **Login**. **d.** Select **Security** > **Certificate Management**. **e.** Click **Upload Certificate** in the Certificate List window. **f.** From the Certificate Name drop-down menu, select **sipproxy-trust**. **g.** Click **Browse** and select **certnew.cer**. **h.** Click **Upload File**.
Step 3	Generate a CSR for Cisco Unified Presence on the Cisco Unified Presence server.	**a.** Select **Security** > **Certificate Management**. **b.** Click **Generate CSR** in the Certificate List window. **c.** From the Certificate Name list, select **sipproxy**. **d.** Click **Generate CSR**.
Step 4	Download the CSR from the Cisco Unified Presence server.	**a.** Select **Security** > **Certificate Management**. **b.** Click **Download CSR** in the Certificate List window. **c.** From the **Certificate Name** list, select **sipproxy**. **d.** Click **Download CSR**. **e.** Click **Save**.

	Task	Procedure
Step 5	Have the root trust of the MS CA sign the CSR	**a.** Copy the certificate request file, sipproxy.csr, to your CA server. **b.** Open the following URL: http://local-server/certserv or http://127.0.0.1/certsrv **c.** Click **Request a certificate**. **d.** Select **advanced certificate request**. **e.** Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**. **f.** Using a text editor like Notepad, open the sip proxy self certificate that you generated. **g.** Copy all information from and including -----**BEGIN CERTIFICATE REQUEST** to and including **END CERTIFICATE REQUEST**----- **h.** Paste the content of the CSR into the Certificate Request text box. **i.** Click **Submit**. **j.** In Administrative Tools, open **Certificate Authority**. **k.** Perform the following actions when the Certificate Authority window displays the request you just submitted under Pending Requests: • Right click on your request. • Select **All Tasks**. **l.** Click **Issue.** **m.** Click **Issued certificates** and verify that your certificate has been issued.

	Task	Procedure
Step 6	Download the signed certificate.	**a.** From Administrative Tools, open Certificate Authority. **b.** Perform the following actions when the pending Certificate Request that you just issued displays in Issued Certificates: – Right click the request that you just issued. – Select **Open**. **c.** Click the **Details** tab. **d.** Click **Copy to File**. **e.** Click **Next** in the Certificate Export Wizard. **f.** Select **Base-64 encoded X.509**. **g.** Click **Next**. **h.** Enter the location where you want to store the certificate and use sipproxy.pem for the certificate name. **i.** Click **Next**. **j.** Review the summary information and click **Finish**. **k.** Copy sipproxy.pem to the computer that you use to administer Cisco Unified Presence.
Step 7	Upload the signed certificate tothe Cisco Unified Presence server as a sipproxy-trust certificate.	See the "Uploading CA-Signed Certificates" section on page 49.
Step 8	Configure the LCS certificate installed on the LCS server.	See the "How to Configure the LCS Certificate Chain" section on page 49.
Step 9	Configure FIPS-compliant algorithms on the LCS server	Configure the LCS server to send TLSv1 with TLS cipher TLS_RSA_WITH_3DES_EDE_CBC_SHA: **a.** Select **Start > Administrative Tools > Domain Controller Security Policy**. **b.** Click **Security Settings** in the console tree. **c.** Perform the following actions: • Click **Local Policies**. • Select **Security Settings**. **d.** In the Details pane, select the **FIPS** security setting. **e.** Modify the security settings and click **OK**.

	Task	Procedure
Step 10	Create a new TLS-PEER Subject on the Cisco Unified Presence server	**a.** Perform the following actions from the Navigation menu on the Cisco Unified Presence Administration login window: – Select **Cisco Unified Presence Administration**. – Click **Go**. **b.** Enter your username and password for Cisco Unified Presence Administration and click **Login**. **c.** Select **Cisco Unified Presence** > **Security** > **TLS Peer Subjects**. **d.** Click **Add New** in the Find and List TLS Peer Subjects window. **e.** For Peer Subject Name, enter the subject CN of the certificate that the LCS server presents. **f.** For Description, enter the name of the LCS server. **g.** Click **Save**.
Step 11	Add the newly created TLS Peer to the Selected TLS Peer Subjects list.	**a.** Select **Cisco Unified Presence** > **Security** > **TLS Context Configuration**. **b.** Click **Find** in the Find and List TLS Contexts window. **c.** Check **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**. **d.** From the list of available TLS ciphers, click **TLS_RSA_WITH_3DES_EDE_CBC_SHA** **e.** Click the down arrow to move it to Selected TLS Ciphers. **f.** From the list of available TLS peer subjects, click the TLS peer subject that you configured **g.** Click the down arrow to move it to Selected TLS Peer Subjects. **h.** Click **Save**.
Step 12	Configure the incoming ACL.	**a.** Select **Cisco Unified Presence** > **Proxy Server** > **Incoming ACL**. **b.** Click **Add New** in the Find and List Allowed Incoming Hosts window. **c.** For Address Pattern, enter ALL or the IP address of the LCS server. **d.** Click **Save**.
Step 13	Restart the SIP Proxy service.	**a.** Log in to Cisco Unified Presence Serviceability Administration. **b.** Select **Tools > Service Activation**. **c.** Restart the Cisco UPS SIP Proxy service.

Office Communications Server 2007 Support

Cisco Unified Presence Release 6.0(2) adds support for Microsoft Client mode (CSTA Integration) with Office Communications Server 2007.

Use this URL to find information about integrating Cisco Unified Presence with Office Communications Server 2007:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/6_0/pbxint/617030nt.pdf

The parameters that are required for Microsoft Office Communications Server 2007 have changed names from Live Communications Server 2005. The TEL URI parameter, defined in Live Communications Server 2005, is the same as the Line URI parameter in Office Communications Server 2007. The Remote Call Control SIP URI parameter, defined in Live Communications Server 2005, is the same as the Server URI parameter in Office Communications Server 2007.

Errors

This section contains information about inaccuracies in the documentation for Cisco Unified Presence Release 6.0(1).

Message Reply in IP Phone Messenger

Problem

The Sending Messages section of the *Cisco IP Phone Messenger Guide* incorrectly suggests that you can use the Msg softkey on the phone to reply to a person who is not in your contact list.

The Msg softkey does not display unless the sender of the message is in the contact list of the receiver.

Solution

To reply to a message using the Msg softkey, add the person who sent the message to your contact list.

Root Certificate URL

Problem

The Microsoft Integration Overview chapter in the *Cisco Unified Presence Deployment Guide* directs users to an incorrect URL to download a root certificate:

- http://127.0.0.1/crtsrv

Solution

Open the following URL to download a root certificate:

- http://127.0.0.1/certsrv

Root Certificate Upload Procedure

The Microsoft Integration Overview chapter in the *Cisco Unified Presence Deployment Guide* contains an obsolete step in the procedure that describes how to upload the root certificate to the Cisco Unified Presence Server.

Step 7 can be ignored.

Cisco Unified PresenceTrust Certificate Filename

The Microsoft Integration Overview chapter in the *Cisco Unified Presence Deployment Guide* does not accurately describe the Trust Certificate Subject CN (Outlook Only) field.

If the CN that you enter contains a space, the space is replaced with an underscore when naming the certificate. During the upload process, a CN of “CA Server,” for example, would equate to entering “CA_Server” in the Trust Certificate Subject CN field.

Incorrect Procedure Sequence

The Microsoft Integration Overview chapter in the *Cisco Unified Presence Deployment Guide* lists the following procedures in an incorrect order:

- Configure a Presence Gateway on the Cisco Unified Presence Server
- Configure the Security Certificate on the Cisco Unified Presence Server

The procedure that describes how to configure the security certificate on the Cisco Unified Presence Server needs to be completed before a presence gateway can be configured on the server. Some of the data fields necessary for the presence gateway are not known until the CA server is installed.

Cisco Unified Presence Upgrade Considerations

The Software Upgrades chapter in the *Cisco Unified Communications Operating System Administration Guide* should state that existing configuration data is not overwritten in an upgrade to Cisco Unified Presence 6.0(1) or later. Once you upgrade to version 6.0(1), you can switch to the new version without reconfiguring your data.

Cisco Unified Presence Release 6.0(3)

This section provides documentation changes that were unavailable when the Cisco Unified Presence Release 6.0(1) documentation suite was released.

- Omissions, page 59
- Errors, page 60

Omissions

This section contains information that may have been left out of the documentation for Cisco Unified Presence Release 6.0(1) or 6.0(2).

Cisco Unified Communications Manager CtiGw Application User Name is Case Sensitive

The caveat referred to above should be added to the *Cisco Unified Presence Administration Guide* and the *Cisco Unified Presence Deployment Guide*.

Related Topics

CTI Gateway Authentication against Cisco Unified Communications Manager is Case-Sensitive, page 30

Restarting the SIP Proxy to Complete Installation of Second Node

You must restart the SIP Proxy service after you configure the second node in a Cisco Unified Presence cluster.

This additional step should be documented as the final step in the "Configuring the Second Node" section of the *Installing Cisco Unified Presence Guide*.

Cisco Unified MeetingPlace Express Unsupported in Cisco Unified Presence

Cisco Unified Presence does not support Cisco Unified MeetingPlace Express. This should be stated in the Meeting Notifications chapter of the *Cisco Unified Presence Administration Guide* and the chapter in the *Cisco IP Phone Messenger for Cisco Unified Presence Guide* that describes Reviewing and Rejoining Meetings.

Configuration of SSL Security Certificate for Meeting Notifications

As you configure meeting notification settings in Cisco Unified Presence Administration, you can check **Use SSL** to specify that the connection to Cisco MeetingPlace will use transport layer security (TLS). The Meeting Notifications chapter of the *Cisco Unified Presence Administration Guide* should include a hyperlink that points users to the security certification configuration procedures, as described in the Microsoft Integration chapter of the *Cisco Unified Presence Deployment Guide*.

Errors

This section contains information about inaccuracies in the documentation for Cisco Unified Presence Release 6.0(2).

Installing CA on the Exchange Server

The Microsoft Integration Overview chapter in the *Cisco Unified Presence Deployment Guide* informs users not to install the CA service on the same computer that is running the Exchange server.

This information note is incorrect. The CA can be installed on the Exchange server.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.