Release Notes for Cisco Unified Presence Release 7.0

March 6, 2012

These release notes describe requirements, restrictions, and caveats for Cisco Unified Presence Release 7.0(1) up to and including Cisco Unified Presence Release 7.0(9).

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

Contents

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

Introduction

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

These release notes describe new features, requirements, restrictions, and caveats for Cisco Unified Presence Release 7.0(x). These release notes are updated for every maintenance release but not for patches or hot fixes.

Before you install Cisco Unified Presence, we recommend that you review the "Related Documentation" section on page 20 for information about the documentation available for Cisco Unified Presence.

System Requirements

- Hardware Server Requirements, page 2
- Server Software Requirements, page 3
- Supported Browsers, page 3

Hardware Server Requirements

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

- One of the following server models:
  - Cisco 7800 Series Media Convergence Server (MCS) listed in the *Hardware and Software Compatibility Information for Cisco Unified Presence Release 7.x*. Go tothe customer-facing DocWiki for the latest information:

    http://docwiki.cisco.com/wiki/Cisco_Unified_Presence%2C_Release_7.x_--_Hardware_and_Software_Compatibility_Information_for_Cisco_Unified_Presence_Release_7.x
  - Cisco-approved, customer-provided third-party server that is the exact equivalent of one of the supported Cisco MCS servers. Go to http://www.cisco.com/go/swonly.
- DVD-ROM drive
- Keyboard, mouse, and monitor

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

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

Related Topics

- How to Upgrade Your Hardware to Cisco Unified Presence Release 7.0(5) or a Higher Release from Legacy Hardware Servers, page 13
- Hardware Caveats, page 48

Server Software Requirements

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

Related Topics

- Installation and Upgrade Notes, page 3

Supported Browsers

Use Microsoft Internet Explorer version 6.0 or a later release to access Cisco Unified Presence Administration, Cisco Unified Serviceability, and Cisco Unified Communications OS Administration. Cisco does not support Mozilla Firefox or other browsers.

Installation and Upgrade Notes

- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3
- New System Installation, page 4
- System Upgrade, page 5
- The Latest Software Upgrades for Cisco Unified Presence on Cisco.com, page 6

Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x)

Cisco Unified Presence Release 7.0(x) supports the following software upgrade paths:

- Cisco Unified Presence Release 1.0(3) to Cisco Unified Presence Release 7.0(1)., 7.0(2), 7.0(3) and 7.0(4).

  See the note below for information on upgrading from Release 1.0(3) and 6.0(1) to Release 7.0(5) or a higher release of Cisco Unified Presence.
- Cisco Unified Presence Release 6.0(x) to Cisco Unified Presence Release 7.0(x).
- Cisco Unified Presence Release 7.0(1) to Cisco Unified Presence Release 7.0(x).

⚠ **Caution** Be aware that you cannot upgrade *directly* from Cisco Unified Presence Release 1.0(3) or earlier to Cisco Unified Presence Release 7.0(5) or a higher 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 7.0(5) from legacy hardware servers.

Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Releases 7.0(5) or Higher Fail with a Sign Error

Problem

If you upgrade from Release 1.0(3) to Release 7.0(5) or a higher release 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 7.0(5) or a higher release of Cisco Unified Presence will fail.

Cause

This condition occurs if you are upgrading from:

- a current active 1.0(3) software release to 7.0(5) or higher software releases.
- a current active 6.0(1) software release to 7.0(5) or higher software releases.

Validation may fail if the file has been tampered with or an error occurred during the download.

Solution

- When upgrading from Release 1.0(3), we recommend that you upgrade to an intermediate Cisco Unified Presence 7.0(x) software release, preferably Release 7.0(4), and then upgrade that version to Release 7.0(5) or a higher 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(2), and then upgrade that version to Release 7.0(5) or a higher release of Cisco Unified Presence.

Related Topics

- How to Upgrade Your Hardware to Cisco Unified Presence Release 7.0(5) or a Higher Release from Legacy Hardware Servers, page 13
- New System Installation, page 4
- System Upgrade, page 5

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/index.shtml or contact your Cisco sales representative.

Each Cisco Unified Presence shipment comes with an installation DVD, which is required for all new installations of a major software release of Cisco Unified Presence, for example, Cisco Unified Presence Release 7.0(1). The Cisco Unified Presence operating system and application software is installed from the installation DVD.

For new installations of the Cisco Unified Presence 7.0(x) application, use the DVD that indicates Cisco Unified Presence 7.0(x) Installation.

Related Topics

- System Upgrade, page 5
- *Installation and Upgrade Guide for Cisco Unified Presence*

System Upgrade

- Upgrade from DVD, page 5
- Upgrade from Cisco.com, page 5

Upgrade from DVD

For major releases of Cisco software, use the DVD provided as part of your Cisco Unified Presence order.

Note When using DVD medias for upgrades, proceed as follows:

- For upgrades from Cisco Unified Presence 6.0(x) to Cisco Unified Presence 7.0(x), use the DVD that indicates Cisco Unified Presence Upgrade (6.0(x) to 7.0(x)). Upgrades from Release 6.0(x) to Release 7.0(x) require the UCSInstall_UCOS_*.sgn.iso file.
- For upgrades from Cisco Unified Presence Release 1.0(x) to Cisco Unified Presence 7.0(x), you must:
  - First install the ciscocm.1x_upgrade.cop.sgn cop file from the Cisco Unified Presence Upgrade DVD Media, "Upgrade from 1.x to 7.0(x)" .
  - Then install cisco-ipt-k9-patch7.0.1.10000-28 from the Cisco Unified Presence Upgrade DVD Media, "Upgrade from 1.x to 7.0(x)".

Caution Cisco Unified Presence does not support direct upgrades from Release 1.0(3) to 7.0(5) or a higher release. If applicable, review the information in this release note about upgrading to Cisco Unified Presence Release 7.0(5) from legacy hardware servers.

Related Topics

- How to Upgrade Your Hardware to Cisco Unified Presence Release 7.0(5) or a Higher Release from Legacy Hardware Servers, page 13

Upgrade from Cisco.com

Cisco does not support downloading major Cisco Unified Presence software releases from Cisco.com, for example, Cisco Unified Presence Release 7.0(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 7.0(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 7.0(x), page 3
- The Latest Software Upgrades for Cisco Unified Presence on Cisco.com, page 6.

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 7.0(1) to 7.0(2), page 6
- Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(3), page 7
- Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(4), page 7
- Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(5), page 8
- Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(6), page 9
- Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(7), page 10
- Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(8), page 10
- Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(9), page 11

Accessing the Upgrade File for Cisco Unified Presence Release 7.0(1) to 7.0(2)

Because of its size, the original UCSInstall ISO file, UCSInstall_UCOS_7.0.1.10000-36.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_7.0.2.10000-36.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.2.10000-36.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_7.0.2.10000-36.sgn.iso_part1of2 UCSInstall_UCOS_7.0.2.10000-36.sgn.iso_part2of2 >
UCSInstall_UCOS_7.0.2.10000-36.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_7.0.2.10000-36.sgn.iso_part1of2+UCSInstall_UCOS_7.0.2.10000-36.sgn.iso_part2of2
UCSInstall_UCOS_7.0.2.10000-36.sgn.iso
```

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

- e87832ba716ad3f0597755936153d65e UCSInstall_UCOS_7.0.2.10000-36.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_7.0.2.10000-36.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5

- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36
- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(3)

Because of its size, the original UCSInstall ISO file, UCSInstall_UCOS_7.0.3.10000-63.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_7.0.3.10000-63.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.3.10000-63.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_7.0.3.10000-63.sgn.iso_part1of2 UCSInstall_UCOS_7.0.3.10000-63.sgn.iso_part2of2 >
UCSInstall_UCOS_7.0.3.10000-63.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_7.0.3.10000-63.sgn.iso_part1of2+UCSInstall_UCOS_7.0.3.10000-63.sgn.iso_part2of2
UCSInstall_UCOS_7.0.3.10000-63.sgn.iso
```

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

- b8530b1230aa6881d281afcd75d282c9 UCSInstall_UCOS_7.0.3.10000-63.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_7.0.3.10000-63.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36
- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(4)

Because of its size, the original UCSInstall ISO file, UCSInstall_UCOS_7.0.4.10000-18.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_7.0.4.10000-18.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.4.10000-18.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_7.0.4.10000-18.sgn.iso_part1of2 UCSInstall_UCOS_7.0.4.10000-18.sgn.iso_part2of2 >
UCSInstall_UCOS_7.0.4.10000-18.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_7.0.4.10000-18.sgn.iso_part1of2+UCSInstall_UCOS_7.0.4.10000-18.sgn.iso_part2of2
UCSInstall_UCOS_7.0.4.10000-18.sgn.iso
```

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

- 057e4d00014a3c69b40f06fadd94239d UCSInstall_UCOS_7.0.4.10000-18.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_7.0.4.10000-18.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36
- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(5)

Because of its size, the original UCSInstall ISO file, UCSInstall_UCOS_7.0.5.10000-18.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_7.0.5.10000-18.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.5.10000-18.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_7.0.5.10000-18.sgn.iso_part1of2 UCSInstall_UCOS_7.0.5.10000-18.sgn.iso_part2of2 >
UCSInstall_UCOS_7.0.5.10000-18.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_7.0.5.10000-18.sgn.iso_part1of2+UCSInstall_UCOS_7.0.5.10000-18.sgn.iso_part2of2
UCSInstall_UCOS_7.0.5.10000-18.sgn.iso
```

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

- 480162b00a49c3e69661c39d3c50331c UCSInstall_UCOS_7.0.5.10000-18.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_7.0.5.10000-18.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36
- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(6)

Because of its size, the original UCSInstall ISO file, UCSInstall_UCOS_7.0.6.10000-17.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_7.0.6.10000-17.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.6.10000-17.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_7.0.6.10000-17.sgn.iso_part1of2 UCSInstall_UCOS_7.0.6.10000-17.sgn.iso_part2of2 >
UCSInstall_UCOS_7.0.6.10000-17.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_7.0.6.10000-17.sgn.iso_part1of2+UCSInstall_UCOS_7.0.6.10000-17.sgn.iso_part2of2
UCSInstall_UCOS_7.0.6.10000-17.sgn.iso
```

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

- 58cd2bfb0777184352249e6aa6887016 UCSInstall_UCOS_7.0.6.10000-17.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_7.0.6.10000-17.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36
- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(7)

Because of its size, the original UCSInstall ISO file, UCSInstall_UCOS_7.0.7.10000-11.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_7.0.7.10000-11.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.7.10000-11.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_7.0.7.10000-11.sgn.iso_part1of2 UCSInstall_UCOS_7.0.7.10000-11.sgn.iso_part2of2 >
UCSInstall_UCOS_7.0.7.10000-11.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_7.0.7.10000-11.sgn.iso_part1of2+UCSInstall_UCOS_7.0.7.10000-11.sgn.iso_part2of2
UCSInstall_UCOS_7.0.7.10000-11.sgn.iso
```

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

- 52c812254be1984f60a707935ff8fae5 UCSInstall_UCOS_7.0.7.10000-11.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_7.0.7.10000-11.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36
- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(8)

Because of its size, the original UCSInstall ISO file, UCSInstall_UCOS_7.0.8.10000-7.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_7.0.8.10000-7.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.8.10000-7.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_7.0.8.10000-7.sgn.iso_part1of2 UCSInstall_UCOS_7.0.8.10000-7.sgn.iso_part2of2 >
UCSInstall_UCOS_7.0.8.10000-7.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_7.0.8.10000-7.sgn.iso_part1of2+UCSInstall_UCOS_7.0.8.10000-7.sgn.iso_part2of2
UCSInstall_UCOS_7.0.8.10000-7.sgn.iso
```

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

- 1dd915ad22f9e2297192f4b2c3be1a5f UCSInstall_UCOS_7.0.8.10000-7.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_7.0.8.10000-7.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36
- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

Accessing the Upgrade File for Cisco Unified Presence Release 7.0(x) to 7.0(9)

Because of its size, the original UCSInstall ISO file, UCSInstall_UCOS_7.0.9.10000-6.sgn.iso, has been divided into two parts that you must download and reunite:

- UCSInstall_UCOS_7.0.9.10000-6.sgn.iso_part1of2
- UCSInstall_UCOS_7.0.9.10000-6.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_7.0.9.10000-6.sgn.iso_part1of2 UCSInstall_UCOS_7.0.9.10000-6.sgn.iso_part2of2 >
UCSInstall_UCOS_7.0.9.10000-6.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_7.0.9.10000-6.sgn.iso_part1of2+UCSInstall_UCOS_7.0.9.10000-6.sgn.iso_part2of2
UCSInstall_UCOS_7.0.9.10000-6.sgn.iso
```

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

- 1ce7227c7d4b7149b5774e1e0b2aa841 UCSInstall_UCOS_7.0.9.10000-6.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_7.0.9.10000-6.sgn.iso) to your FTP or SFTP server.

Related Topics

- Upgrade from Cisco.com, page 5
- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36
- Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

Additional Installation and Upgrade Considerations

- Perform Cisco Unified Presence 7.0 Upgrade Before Cisco Unified Communications Manager 6x and 7.x Upgrade, page 12
- How to Upgrade Your Hardware to Cisco Unified Presence Release 7.0(5) or a Higher Release from Legacy Hardware Servers, page 13
- Upgrade Consideration for Multi-Node Feature, page 18
- Post-Upgrade Requirement for Cisco Unified Presence 7.0(4) with Cisco Unified Communications Manager Versions Prior to 7.1(2), page 19

Perform Cisco Unified Presence 7.0 Upgrade Before Cisco Unified Communications Manager 6x and 7.x Upgrade

You must perform the Cisco Unified Presence Release 7.0 upgrade *before* you perform the Cisco Unified Communications Manager Release 6.x and 7.x upgrade. Cisco does not support synchronization between Cisco Unified Communications Manager Release 6.x and 7.x running Cisco Unified Presence Release 1.x.

Note After upgrading Cisco Unified Communications Manager to 6.x or 7.x you must stop and then restart the Cisco UP Sync Agent service. Select **Cisco Unified Serviceability> Tools > Control Center - Feature Services.**

How to Upgrade Your Hardware to Cisco Unified Presence Release 7.0(5) or a Higher Release from Legacy Hardware Servers

You cannot directly upgrade to Cisco Unified Presence Release 7.0(5) from Cisco Unified Presence Release 1.0(3). We recommend that you upgrade to an intermediate 7.0(x) release of Cisco Unified Presence (Release 7.0(4) is best), and then upgrade that version to Release 7.0(5) 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 7.0(4) 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 7.0(4). 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 7.0(4) on a new hardware platform.
4. Migrate your data without changing your configuration.

Prerequisites

Ensure that you have the following prerequisites:

- Release 7.0(4) 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 7.0(4).
- New Cisco Unified Presence 7.0(4) 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 Presence 1.0(3) Server Upgraded to 7.0(4)

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. Select **Go**.

Step 2 Sign 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 7.0(4)	a. Select **Backup > Backup Device**. b. Select **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. Select **Save** to update these settings.
Already set up on your Cisco Unified Presence 1.0(3) server upgraded to 7.0(4)	a. Verify the following field values in the Select Destination area: • Path name: your entry must point to where the Release 7.0(4) 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 Select **Start Backup** to start the manual backup.

Step 8 When the backup is complete, check under the **Path name** for successfully backed up files with names similar to these:

- 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 15

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. Select **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 Select **Shutdown** to shut down the system.

Step 4 Monitor the Cisco Unified Presence server console and wait until it powers down.

Step 5 Install Cisco Unified Presence Release 7.0(4) on a new hardware platform using the same hostname and IP address.

Troubleshooting Tips

Press the On/Off switch on the Cisco Unified Presence server only if the server does not power down.

What To Do Next

Migrating Data To a Cisco Unified Presence 7.0(4) Server Installed on New Hardware, page 16

Migrating Data To a Cisco Unified Presence 7.0(4) 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. Select **Go**.

Step 2 Sign 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 Select **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 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

Step 7 Select **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 Select **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 Select **Next**. The Restore Wizard Step 3 window displays.

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

Step 14 Select **Next**.

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

Step 16 Select **Restore**.

What To Do Next

Restarting the System, page 17

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. Select **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 Select **Restart**.

What To Do Next

Uploading the License File, page 17

Uploading the License File

Procedure

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

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

Step 3 Select **Upload.**

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

Step 5 Select **Upload**.

Step 6 Select **Continue**.

What To Do Next

Activating Feature Services, page 17

Activating Feature Services

Procedure

Step 1 Perform the following actions:

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

b. Select **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. Select **Go**.

Step 4 Activate the following services by checking the check box next to each one:

- SIP Proxy
- Presence Engine
- Sync Agent

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

What To Do Next

Verifying System Configuration, page 18

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. Select **Go.**

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

Upgrade Consideration for Multi-Node Feature

If your configuration meets the following criteria, then you must take some additional steps to get up-and-running:

- Your initial Cisco Unified Presence installation was software release 1.0.3 on an MCS 7845 H1/I1 platform
- You want to upgrade from release 1.03 to release 7.0(x), or from release 1.0.3 to release 6.0(x) to release 7.0(x)
- You want to support the multi-node feature using this platform

If you meet these criteria, follow these upgrade guidelines to use the /spare partition to support a larger user database:

1. Perform an upgrade to release 7.0(x).
2. Perform a DRS backup.
3. Perform a fresh installation of release 7.0(x) on the publisher and subscriber nodes (if any).
4. Perform a DRS restore.

For further information on performing backup and restore procedures on Cisco Unified Presence, see the *Disaster Recovery System Administration Guide for Cisco Unified Presence Release 7.0.*

Post-Upgrade Requirement for Cisco Unified Presence 7.0(4) with Cisco Unified Communications Manager Versions Prior to 7.1(2)

If you are upgrading to Cisco Unified Presence 7.0(4) while using Cisco Unified Communications Manager version prior to 7.1(2), the Disaster Recovery System will not work after upgrading (see also, CSCsz44417).

When you attempt to back up a device or provision a new device, the Backup Device page reports: "Local Agent is not responding. This may be due to Master or Local Agent being down."

To avoid this issue and to continue backing up your data, follow this procedure immediately after upgrading to Cisco Unified Presence 7.0(4):

Procedure

Step 1 Sign in to Cisco Unified Communications Operating System Administration on the Cisco Unified Presence publisher.

Step 2 Select **Security > Certificate Management**.

Step 3 Enter ipsec.pem and select **Find**.

Step 4 Select **Download**.

Step 5 Select **Save**.

After downloading the ipsec.pem file, you then need to upload it to each node of the cluster, including the publisher.

Step 6 Select **Security > Certificate Management**.

Step 7 Select **Upload Certificate**.

Step 8 Select **ipsec-trust** from the Certificate Name list.

Step 9 Select **Browse** and navigate to the file.

Step 10 Select **Upload File** and repeat for each node of the cluster.

Step 11 Restart the DRF Local Agent on all nodes using Cisco Unified Serviceability.

Limitations and Restrictions

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

Table 1 Closed Caveats for Cisco Unified Presence

Identifier	Severity	Component	Headline
CSCsx10412	4	ctigw	MOC-RCC/CUP Unable to Detect That Controlled Device is Unregistered
CSCth95277	3	intercluster	ICSA SQL error when CUCM publisher trunk not used

Related Documentation

The complete documentation set, with the latest information for Release 7.0 through Release 7.0(9), is now available for administrators of Cisco Unified Presence on DocWiki, at this location:

http://docwiki.cisco.com/wiki/Cisco_Unified_Presence%2C_Release_7.x

To search for documentation on the DocWiki, we recommend using Google. Go to Google.com and enter this: <*your search term*> site:docwiki.cisco.com. where <*your search term*> is the term you want to search.

Cisco community members with CCO passwords can contribute expertise to articles and exchange ideas on the Discussion page associated with each article. For more information, click the About DocWiki link at the bottom of any page on the DocWiki.

New and Changed Information

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

- About Cisco Unified Presence Release 7.0(1), page 20
- About Cisco Unified Presence Release 7.0(2), page 21
- About Cisco Unified Presence Release 7.0(3), page 21
- About Cisco Unified Presence Release 7.0(4), page 23
- About Cisco Unified Presence Release 7.0(5), page 30
- About Cisco Unified Presence Release 7.0(6), page 31
- About Cisco Unified Presence Release 7.0(9), page 31

About Cisco Unified Presence Release 7.0(1)

The following sections describe new features and changes that are pertinent to Cisco Unified Presence, Release 7.0(1). The sections may include configuration tips for the administrator, information about users, and where to find more information.

- Copyright Information, page 20
- Support Status for Cisco Unified Presence Interface, page 21
- Support Status for Transport Layer Security (TLS) in SIP Trunk, page 21

Copyright Information

Portions of this software product are governed by certain open source and third-party licenses. For more information and acknowledgements of copyright, see the *Licensing Information for Cisco Unified Presence* at the following URL:

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

Support Status for Cisco Unified Presence Interface

Please consult Cisco Developer Community for supported Cisco Unified Presence interfaces at the following URL:

http://developer.cisco.com/web/cdc/home;jsessionid=B2EE8D3CDB731A1709AC8F88349ACD28.liferay-portal1

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

TLS cannot be used to interface between Cisco Unified Presence Release 7.0 and the Cisco Unified Communications Manager SIP trunk.

About Cisco Unified Presence Release 7.0(2)

The following sections describe new features and changes that are pertinent to Cisco Unified Presence, Release 7.0(2). The sections may include configuration tips for the administrator, information about users, and where to find more information.

- Support for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator, page 21
- Active-Standby High Availability Support, page 21

Support for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator

This release supports the integration of Cisco Unified Presence with Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator.

Active-Standby High Availability Support

In this release, Cisco Unified Presence has added Active-Standby as a High Availability (HA) deployment option. The SyncAgent service parameter, User Dispersal Mode, now contains the new option for Active-Standby.

Active-Standby support allows an administrator to configure a primary Cisco Unified Presence node to contain 100% of the users for the subcluster while the back-up node has no users. The back-up node is a hot standby node. In the event of a failure, users will fail over to the back-up node. The back-up node is idle except when a failover has occurred.

Auto-assignment of users will honor this configuration option. In addition, administrators will be able to manually assign users using Active-Standby mode. User rebalancing is also provided and fully supports Active-Standby.

The “Balanced” HA mode remains fully supported and is integrated in the UI via the **Rebalance** button in the System Topology window.

About Cisco Unified Presence Release 7.0(3)

The following sections describe new features and changes that are pertinent to Cisco Unified Presence, Release 7.0(3). The sections may include configuration tips for the administrator, information about users, and where to find more information.

- Support for Integration with Cisco WebEx Meeting Center, page 22

Support for Integration with Cisco WebEx Meeting Center

This feature enables Cisco Unified Personal Communicator clients to use Cisco WebEx Meeting Center for web collaboration. You can configure Cisco Unified Presence to integrate with Cisco WebEx servers, which allows users of Cisco Unified Personal Communicator to launch an unscheduled web conference from the audio or video conversation window.

Simplification of Microsoft Exchange Certificate Configuration

Cisco Unified Presence Release 7.0(3) allows you to perform certificate configuration for the Presence Exchange Gateway in Cisco Unified Presence Administration. You can access a Certificate Chain viewer, and view or configure the certificates according to the current status of the Exchange SSL connection and certificate results.

Support for Microsoft Exchange Integration with Windows 2008

This release of Cisco Unified Presence allows for the integration of Microsoft Exchange with Active Directory 2008 and Windows server 2008.

Support for Redundancy in Interdomain Federation

For redundancy and high availability purposes, you can now deploy a load balancer in the federated network, located between Cisco Unified Presence and Cisco Adaptive Security Appliance. The load balancer terminates incoming TLS connections from Cisco Adaptive Security Appliance, and initiates a new TLS connection to route the content to the appropriate backend Cisco Unified Presence server.

Support for Email Address in Interdomain Federation

In this Cisco Unified Presence release, you can use an email address for interdomain federation. You can change the SIP URI of each user from userid@domain to an email address (or vice versa) during federation with a foreign enterprise.

No Longer Required to Add Cisco Unified Presence as an Application server on Cisco Unified Communications Manager

This release eliminates a previously valid configuration step in Cisco Unified Presence. If you configure the publisher node, then you do not need to add Cisco Unified Presence server nodes to the Cisco Unified Communications Manager Application Server list (**System > Application Server** in Cisco Unified Communications Manager Administration).

This step is no longer required because Cisco Unified Presence now completes it programmatically via a remote AXL call on the System Topology page. When the administrator adds a new node on the System Topology page, the node is automatically added to the Cisco Unified Communications Manager Application Server list. Conversely, if a node is removed from Cisco Unified Presence via the System Topology page, the node is automatically removed from the Cisco Unified Communications Manager Application Server list.

About Cisco Unified Presence Release 7.0(4)

The following sections describe new features and changes that are pertinent to Cisco Unified Presence, Release 7.0(4). The sections may include configuration tips for the administrator, information about users, and where to find more information.

- Post-Upgrade Requirement for Cisco Unified Presence 7.0(4) with Cisco Unified Communications Manager Versions Prior to 7.1(2), page 23
- Upgrade Process Takes Longer to Complete, page 23
- Upgrade to Operating System and Tomcat Web Server Versions, page 26
- Cisco Adaptive Security Appliance Version 8.2 Required for Federation Integration, page 26
- Update to the Microsoft Office Communicator Call Control Feature, page 26
- Creating a Customized Log-on Message, page 27
- Support for OpenLDAP Servers, page 27
- Server-Side Failback for Cisco Unified Personal Communicator Clients, page 28
- SIP Proxy Restart Required, page 28
- Changes and Additions to the Command Line Interface Commands, page 28
- Multi-Device Remote Call Control (RCC) Available as an Application Plug-in, page 29

Post-Upgrade Requirement for Cisco Unified Presence 7.0(4) with Cisco Unified Communications Manager Versions Prior to 7.1(2)

If you are upgrading to Cisco Unified Presence 7.0(4) while using Cisco Unified Communications Manager version prior to 7.1(2), the Disaster Recovery System will not work initially after upgrading. To prevent this issue, refer to the "Post-Upgrade Requirement for Cisco Unified Presence 7.0(4) with Cisco Unified Communications Manager Versions Prior to 7.1(2)" section on page 19 for details.

Upgrade Process Takes Longer to Complete

To preserve system stability during upgrades, the system throttles the upgrade process, which may take considerably longer to complete in Cisco Unified Presence 7.0(1) and later than it did in earlier releases.

However, if the upgrade process is taking much longer than you would like, you can disable throttling. Although disabling throttling decreases the time it takes to perform the upgrade, it may degrade system performance. For more information about throttling and the causes of slow upgrades, see the "Effects of I/O Throttling" section on page 24. To disable throttling, use the following command in the CLI before you start the upgrade: **utils iothrottle disable**

Note Note: If you want to reenable throttling after you start the upgrade, you must cancel the upgrade, reenable throttling, and then restart the upgrade.

Effects of I/O Throttling

This section describes how throttling affects the upgrade process, identifies possible causes of slow or stalled upgrades, and provides actions you can take to speed up the upgrade.

This section contains the following information:

- Overview, page 24
- Disabling Throttling, page 24
- Server Models, page 24
- Write-Cache, page 24

Overview

Throttling may cause the upgrade to take longer. Throttling is enabled by default and is necessary if you perform the upgrade during normal business hours.

Disabling Throttling

To disable throttling, use the following command: **utils iothrottle disable**

Note Note: If you want to reenable throttling after you start the upgrade, you must cancel the upgrade, reenable throttling, and then restart the upgrade.

Server Models

The Server model you have also impacts the upgrade speed. Upgrades on servers that have SATA hard drives, such as MCS-7816 and MCS-7825, take longer than servers with SAS/SCSI hard drives, such as MCS-7835 and MCS-7845.

Write-Cache

A disabled write-cache on the server also causes the upgrade process to run more slowly. Multiple factors can cause the write-cache to become disabled, including dead batteries on older servers.

Before starting an upgrade, verify the status of the write-cache on the MCS-7835/45 disk controllers. You do not need to verify the write-cache status on the MCS-7816, MCS-7825 servers. To verify write-cache status, access the Cisco Unified Operating System Administration, and select **Show > Hardware**.

If you determine that your write-cache is disabled because of a dead battery, you need to replace the hard disk controller cache battery. Follow your local support procedures to get this battery replaced.

See the following examples of output from the **Show > Hardware** menu for details on determining the battery and write-back cache status.

In the following example write-cache is enabled. The example indicates that 50 percent of the cache is reserved for write and 50 percent of the cache is reserved for read. If the write-cache was disabled, 100 percent of the cache would be reserved for read or the Cache Status would not equal “OK”. Also, the battery count equals “1”. If the controller battery was dead or missing, it would indicate “0”.

Example 1 7835/45-H1 and 7835/45-H2 Servers with Write-Cache Enabled

```
-------------------------------
RAID Details      :

Smart Array 6i in Slot 0
   Bus Interface: PCI
   Slot: 0
   Cache Serial Number: P75B20C9SR642P
   RAID 6 (ADG) Status: Disabled
   Controller Status: OK
   Chassis Slot:
   Hardware Revision: Rev B
   Firmware Version: 2.80
   Rebuild Priority: Low
   Expand Priority: Low
   Surface Scan Delay: 15 sec
   Cache Board Present: True
   Cache Status: OK
   Accelerator Ratio: 50% Read / 50% Write
   Total Cache Size: 192 MB
   Battery Pack Count: 1
   Battery Status: OK
   SATA NCQ Supported: False
```

The following example indicates that the battery status is enabled and that the write-cache mode is enabled.

Example 2 7835/45-I2 Servers with Write-Cache Enabled

```
----------
RAID Details      :
Controllers found: 1

----------------------------------------------------------------------
Controller information
----------------------------------------------------------------------
   Controller Status                    : Okay
   Channel description                  : SAS/SATA
   Controller Model                     : IBM ServeRAID 8k
   Controller Serial Number             : 20ee0001
   Physical Slot                        : 0
   Copyback                             : Disabled
   Data scrubbing                       : Enabled
   Defunct disk drive count             : 0
   Logical drives/Offline/Critical      : 2/0/0
   ---------------------------------------------------
   Controller Version Information
   ---------------------------------------------------
   BIOS                                 : 5.2-0 (15421)
   Firmware                             : 5.2-0 (15421)
   Driver                               : 1.1-5 (2412)
   Boot Flash                           : 5.1-0 (15421)
   ---------------------------------------------------
   Controller Battery Information
   ---------------------------------------------------
   Status                               : Okay
   Over temperature                     : No
   Capacity remaining                   : 100 percent
   Time remaining (at current draw)     : 4 days, 18 hours, 40 minutes
   ---------------------------------------------------
   Controller Vital Product Data
   ---------------------------------------------------
   VPD Assigned#                       : 25R8075
   EC Version#                         : J85096
   Controller FRU#                     : 25R8076
   Battery FRU#                        : 25R8088

----------------------------------------------------------------------
Logical drive information
----------------------------------------------------------------------
Logical drive number 1
   Logical drive name                  : Logical Drive 1
   RAID level                          : 1
   Status of logical drive             : Okay
   Size                                : 69900 MB
   Read-cache mode                     : Enabled
   Write-cache mode                    : Enabled (write-back)
   Write-cache setting                 : Enabled (write-back) when protected by battery
   Number of chunks                    : 2
   Drive(s) (Channel,Device)           : 0,0 0,1
Logical drive number 2
   Logical drive name                  : Logical Drive 2
   RAID level                          : 1
   Status of logical drive             : Okay
   Size                                : 69900 MB
   Read-cache mode                     : Enabled
   Write-cache mode                    : Enabled (write-back)
   Write-cache setting                 : Enabled (write-back) when protected by battery
   Number of chunks                    : 2
   Drive(s) (Channel,Device)           : 0,2 0,3
```

Upgrade to Operating System and Tomcat Web Server Versions

After upgrading to Cisco Unified Presence Release 7.0(4), the Tomcat web server is version 6.0.18, and the underlying operating system is now RHEL4 U6, which aligns with Cisco Unified Communications Manager 7.1(2).

Cisco Adaptive Security Appliance Version 8.2 Required for Federation Integration

Cisco Unified Presence Release 7.0(4) requires Cisco Adaptive Security Appliance Version 8.2 for interdomain federation integration. This update applies to the *Integration Guide for Configuring Cisco Unified Presence Release 7.0 for Interdomain Federation*.

Update to the Microsoft Office Communicator Call Control Feature

Cisco Unified Presence Release 7.0(4) includes an update to the Microsoft Office Communicator call control feature that impacts users. This update applies to the *User Guide for Cisco IP Phone Messenger and Cisco Unified Presence Release 7.0*

Previously, each time users switched between devices using the Microsoft Office Communicator, they needed to sign out of Microsoft Office Communicator and sign in again for the change to take effect. With this update, the switch takes place immediately, and users only need to sign out and in again after the first time they select a device.

Procedure

Step 1 On the Phone Selection screen on the Microsoft Office Communicator client, enter your username for the Cisco Unified Presence end user interface provided by your system administrator.

Step 2 Enter your password for the Cisco Unified Presence end user interface, provided by your system administrator.

Step 3 Select **Login**.

Step 4 Select a phone device to control from the Phone Selection menu.

Step 5 Select **Change**.

Creating a Customized Log-on Message

You can upload a text file that contains a customized log-on message that appears in each of the Cisco Unified Presence applications administrative interfaces.

Procedure

Step 1 Sign in to Cisco Unified Communications Operating System Administration.

Step 2 Select **Software Upgrades > Customized Logon Message**.

Step 3 Select **Browse** to select the text file you want to upload.

Note Text files are the only supported format and must be smaller than 10KB.

Step 4 Select **Upload File**.

Step 5 To revert to the default log-on message, click **Delete**.

Support for OpenLDAP Servers

Cisco Unified Presence 7.0(4) provides support for OpenLDAP servers for use with Cisco Unified Personal Communicator. This update applies to the *Configuration and Maintenance Guide for Cisco Unified Presence Release 7.0* and the *Deployment Guide for Cisco Unified Presence Release 7.0.1, 7.0.2 and 7.0.3*.

Note If you are specifying more than one LDAP server for failover support, the servers must all be of the same type (all Microsoft Active Directory, all Netscape, or all Sun One Directory). The LDAP attribute schema must be the same on all servers.

Procedure

Step 1 Sign in to Cisco Unified Presence Administration.

Step 2 Select **Application > Cisco Unified Personal Communicator > Settings**.

Step 3 Select the appropriate Directory Server Type settings for Cisco Unified Personal Communicator as described in Table 1-2.

Table 1-2 Cisco Unified Personal Communicator Configuration Settings

Field	Description
Directory Server Type	• Microsoft Active Directory—choose this option for Microsoft Active Directory servers • Netscape or Sun ONE LDAP—choose this option for Netscape, Sun ONE LDAP, and OpenLDAP servers

Server-Side Failback for Cisco Unified Personal Communicator Clients

Cisco Unified Presence 7.0(4) provides server-side failback as a new scalability and high-availability feature. Server-side failback uses the same throttle mechanism as server failover. This feature detects when a failed Cisco Unified Presence server in a high-availability deployment comes back in service. It then sends terminating notify messages to Cisco Unified Personal Communicator clients that are failed over to initiate failback to their home node. Also, if a user is moved between nodes in the subcluster, the Cisco Unified Presence server sends terminating notify messages, and the client will sign out and sign in to the new node. To balance the load between two nodes in the subcluster, you can assign the users equally in each node.

SIP Proxy Restart Required

These situations require that you restart the SIP proxy:

- When changing the control CTI address of a desk phone (CSCsz45780)
- To control MOC-RC C after an L2 upgrade (CSCsz43829)

Procedure

Step 1 **Select Navigation > Cisco Unified Serviceability** from the menu in the upper, right corner of the Cisco Unified Presence main window and select **Go**.

Step 2 Select **Tools > Control Center > Feature Services**.

Step 3 Select the appropriate Cisco Unified Presence server.

Step 4 Select the radio button next to **Cisco UP SIP Proxy**.

Step 5 Select **Restart**.

Step 6 Select **OK**. when a message indicates that restarting may take a while.

Changes and Additions to the Command Line Interface Commands

Cisco Unified Presence 7.0(4) provides some changes and additions to the command line interface commands. This update applies to the *Cisco Unified Communications Operating System Maintenance Guide for Cisco Unified Presence*.

utils core list

This command lists all existing core files.

Command Syntax

utils core [active | inactive] list

Parameters

- **active**—specifies an active version
- **inactive**—specifies an inactive version

utils core analyze

This command generates a backtrace for the specified core file, a thread list, and the current value of all CPU registers.

Command Syntax

utils core [active | inactive] analyze *core file name*

Parameters

- **active**—specifies an active version
- **inactive**—specifies an inactive version
- *core file name* specifies the name of a core file.

Usage Guidelines

The command creates a file of the same name as the core file, with a .txt extension, in the same directory as the core file. This command works only on the active partition.

utils nscd restart

This command restarts the network service cache daemon (nscd).

Command Syntax

utils nscd restart

utils nscd status

This command tests the network service cache daemon (nscd).

Command Syntax

utils nscd status

Multi-Device Remote Call Control (RCC) Available as an Application Plug-in

Cisco Unified Presence 7.0(3) provided the Microsoft Office Communicator (MOC) RCC feature, which is a plug-in for the MOC client that allows the user to select any phone device that they wish to control via MOC. Instead of building functionality into MOC itself, this feature makes use of a MOC plug-in URL that points to Cisco Unified Presence at the back end. Users control the device selection from within their MOC client.

In Cisco Unified Presence 7.0(3) this was only available as a download from Cisco.com. However, you can now download the MOC RCC plugin installer directly from Cisco Unified Presence Administration.

Procedure

Step 1 Select **Application > Plugins**.

Step 2 To find all available plugins, ensure that the dialog boxes are empty and click **Find**.

Step 3 Select the **Download** link to download the **Cisco Unified Presence MOC Remote Call Control Plugin**.

Step 4 Follow the instructions in the installation wizard to complete the installation.

About Cisco Unified Presence Release 7.0(5)

- Cisco Unified Presence Evaluation Mode, page 30
- Support for Clustering over WAN Deployment, page 30
- Support for Microsoft Office Communications Server 2007 Release 2, page 30
- Support for Microsoft ADAM Directory Service, page 31
- Support for Multilingual Calendaring Integration, page 31

Cisco Unified Presence Evaluation Mode

Immediately following a fresh installation, Cisco Unified Presence 7.0(5) now defaults to an Evaluation mode for 90 days. This is a trial assessment period, during which an organization can use or "run" a Cisco Unified Presence server without requiring a server license. Users in that organization, who are already configured on Cisco Unified Communications Manager, can access Cisco Unified Presence and be configured to use Cisco Unified Personal Communicator, without requiring the necessary user licenses (DLUs).

A Licensing Warning(s) message, in Cisco Unified Presence Administration, informs you whether the Evaluation license has already expired or the number of days remaining to expiry. You can upload the license to Cisco Unified Presence before or after the trial evaluation period ends. After Evaluation mode expires, you no longer have access to Cisco Unified Presence functionality.

Support for Clustering over WAN Deployment

Cisco Unified Presence Release 7.0(5) supports Clustering over WAN for intracluster and intercluster deployments. For both these types of deployments, Cisco recommends a minimum of a five megabyte bandwidth with an eighty millisecond round-trip latency. For intracluster deployments over WAN, Cisco Unified Presence supports only a single subcluster geographically split over WAN.

Support for Microsoft Office Communications Server 2007 Release 2

Cisco Unified Presence Release 7.0(5) supports the integration of Cisco Unified Presence with Microsoft Office Communications Server 2007 Release 2 for the remote call control feature, and the interdomain federation feature.

Support for Microsoft ADAM Directory Service

Cisco Unified Presence Release 7.0(5) provides support for the Active Directory Application Mode (ADAM) service. This is for use with the Cisco Unified Personal Communicator client.

Support for Multilingual Calendaring Integration

This software release of Cisco Unified Presence allows you to configure your Microsoft Exchange deployment to support multiple languages. There is no limit to the number of supported languages. You configure Cisco Unified Communications Manager and Cisco Unified Presence to support the user locales that you require in your calendaring integration.

About Cisco Unified Presence Release 7.0(6)

- Enhanced Wildcard Usage in Static Route Configuration, page 31

Enhanced Wildcard Usage in Static Route Configuration

This release provides support for embedded '.' wildcard characters in static routes based on a route embed template.

About Cisco Unified Presence Release 7.0(9)

- Support for Cisco Unified Customer Voice Portal (CVP), page 31

Support for Cisco Unified Customer Voice Portal (CVP)

The following configuration must be configured for CVP support in this release.

Procedure

Step 1 Select **System > Service Parameter** in Cisco Unified Presence Administration.

Step 2 Select the required server.

Step 3 Select the Cisco UP SIP Proxy service.

Step 4 Select **Off** for the Add Record-Route Header option in the SIP Parameters section to turn off this option.

Step 5 Select **Off** for the Route Failure option in the Routing Parameters section to turn off this option.

Step 6 Select **Save**.

Troubleshooting Tips

When configuring static routes, we recommend that you use the TCP protocol to route messages. To do this, select **Presence > Routing > Static Routes** in Cisco Unified Presence Administration.

Important Notes

About Cisco Unified Presence Release 7.0(1)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 7.0(1).

Availability Status of Users Does Not Display after Change to Proxy Domain

Problem

If you change the Proxy Domain settings on Cisco Unified Presence while users are signed into Cisco Unified Personal Communicator, the availability status does not display on the client.

Cause

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

Solution

Before you change the Proxy Domain settings on Cisco Unified Presence, make sure that all users are fully signed out of their Cisco Unified Personal Communicator client.

SIP Trunk Listening Port Change on Cisco Unified Presence Must be Replicated on Cisco Unified Communications Manager

Beginning with Cisco Unified Presence Release 7.0, the SIP Trunk listening port has been changed to 5060. Therefore, the SIP Trunk destination port must also change to 5060 on the Cisco Unified Communications Manager server.

Recommendations for ASA in Interdomain Federation

It is recommended that you allow ASA to reset idle connections after an hour.

Procedure

Step 1 Enter the following configuration mode command on ASA:

```
enter config t
```

Step 2 Enter the following command to add the access list:

```
access-list CUPS_SERVER extended permit tcp any any eq5061
```

Step 3 Enter the following command to add the class-map that references the access-list:

```
class-map CUPS_SERVER
match access-list CUPS_SERVER
```

Step 4 Enter the following command to add the class-map to the policy-map global-policy:

```
policy-map global_policy
class CUPS_SERVER
set connection timeout tcp 1:00:00 reset
```

Step 5 Save with a write memory.

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 user names 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 (select **Application > Deskphone Control > Settings**), ensure that you enter the exact same application CTI Gateway username and password that you configured on Cisco Unified Communications Manager.

Restarting the Tomcat Web Server to Complete Certificate Exchange

A self-signed certificate is generated on the Tomcat web server during its installation. The certificate is also migrated during upgrades. You must restart the Tomcat web server after you upload or regenerate the Tomcat certificate on Cisco Unified Presence.

You can load certificates in Cisco Unified Operating System Administration (select **Security > Certificate Management**).

Known Issues with Cisco IP Phone Messenger

- Limitation with Cisco IP Phone Messenger in a Multi-Node Cisco Unified Presence Cluster, page 34
- Cisco IP Phone Messenger Recreates a Deleted Group in Error, page 35

Limitation with Cisco IP Phone Messenger in a Multi-Node Cisco Unified Presence Cluster

Problem

If administrators or users use the wrong XML service for Cisco IP Phone Messenger, user sign in to the phone device fails. An error message informs the user that they may be trying to sign in to a node that is not their home node.

Cause

This condition occurs if a multinode Cisco Unified Presence cluster is deployed, and a user is assigned (or re-assigned) to another node.

Solution

You need to set up the Cisco IP Phone Messenger service so the user can sign in to the correct node.

Perform the following actions before logging into Cisco IP Phone Messenger:

If you are the:	Action
Administrator of Cisco IP Phone Messenger	In Cisco Unified Communications Manager Administration, configure the XML services for Cisco IP Phone Messenger. For example, in a four-node Cisco Unified Presence cluster, configure four XML services for Cisco IP Phone Messenger and have users subscribe to the service that points to their home node. If you rehome a user to another Cisco Unified Presence node, unsubscribe your user from the old Cisco IP Phone Messenger service and resubscribe them to the correct XML service.
User of Cisco IP Phone Messenger	Select the IPPM service that runs on the Cisco Unified Presence home node.

Cisco IP Phone Messenger Recreates a Deleted Group in Error

Problem

Cisco IP Phone Messenger recreates the “General” group that has been previously deleted in Cisco Unified Personal Communicator. This occurs when an end user configured for both Cisco Unified Personal Communicator and Cisco IP Phone Messenger:

- Deletes the default "General" group from Cisco Unified Personal Communicator
- Adds a contact in Cisco IP Phone Messenger

Cause

Cisco IP Phone Messenger does not expose group creation or contact addition into specific groups. Cisco IP Phone Messenger looks for contact groups to have an "isdefault" flag set to true. If a group does not have the "isdefault" flag set to true, then Cisco IP Phone Messenger will recreate the General group.

Solution

Instead of deleting the General group in Cisco Unified Personal Communicator, rename it.

Client Config Interface is Incompatible with Latest Axis Library

Problem

Version 1.4 of Axis Library includes an attribute, mustUnderstand, in all requests. The Client Config Interface rejects these requests. To resolve the issue, you can change the xsd/wsdl that describes the interface but it will require you to regenerate stubs. This could cause compatibility issues

Solution

When using Cisco Unified Presence APIs (over SOAP), do not use the latest library available, Axis Library version 1.4. Instead, use Axis Library version 1.2.

Unknown Service Status if Admin Password Field Contains the “@” Character

Problem

If your Administrator password contains the character "@" (for example, cisco@123), the status of all the services on both the Publisher and the Subscriber nodes shows as UNKNOWN under **System > Topology**.

Cause

The service status displays as UNKNOWN if you enter the "@" character in the Administrator Password field.

Solution

Remove the character "@" from the password field.

Cisco Unified Presence Does Not Support Multiple Logins to Microsoft Office Communicator (MOC)

Multiple MOC logins cause the interaction of Cisco Unified Presence RCC features to become unreliable. We recommend that you do not sign in simultaneously to two different MOC clients using the same login ID.

About Cisco Unified Presence Release 7.0(3)

- Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases, page 36

Configuring Application Server on Cisco Unified Communications Manager is Automatic from Cisco Unified Presence Release 7.0.3 and Higher Releases

In this release and higher releases of Cisco Unified Presence, you no longer have to manually add Cisco Unified Presence as an Application Server on Cisco Unified Communications Manager. For more information, see

http://docwiki.cisco.com/wiki/Cisco_Unified_Presence,_Release_7.x_--_Configuring_the_Presence_Service_Parameter

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 installation. Alternatively, use a Mozilla-based browser such as Firefox (any version) to download the patch file.

Expiry of Receive-As Account Password Prompts Error Message

When the password for the Receive-As account expires, the Cisco Unified Presence server displays a "440 Login Timeout" message. This message is very generic and does *not* enable the administrator to determine the real cause of the error. This issue applies to all versions of Micrsoft Exchange.

404 Login Timeout Message

12/01/2008 13:53:51.799 EPE|system.pe.pa.owa.backend 2056682 ERROR Exchange Server Transaction Failed: SUBSCRIBE

sip:dell@exch2k7-front:443 440 Login Timeout - clear calendar information

Mailbox Store and Client Access Server Recommendation

If you deploy Microsoft Exchange 2007, we recommend that you do *not* install the mailbox role on the server running Client Access Server. When the mailbox role is installed on the same server as Client Access Server, it has been observed that calendaring presence does not work correctly. Use a standalone CAS.

SSL Connection Failure between Cisco Unified Presence Server and Exchange 2003 Server

Problem

If you are deploying Cisco Unified Presence with Microsoft Exchange 2003 and Windows Server 2003, the Exchange SSL Connection/Certificate Verification between the servers may fail. Select **Presence > Gateways** in Cisco Unified Presence Administration for confirmation. If the SSL connection fails:

- Presence status is not obtained correctly on Cisco Unified Personal Communicator.
- Users can *not* search for other users on the LDAP server on Cisco Unified Personal Communicator.

Cause

The cause of this behavior is not known.

Solution

You can perform a workaroundon the LDAP server (global catalog), as follows:

Procedure

Step 1 Navigate to the following location on the LDAP server:

Manage Your Server > Remote Access/VPN Server > Manage this remote access/VPN server

Step 2 Double-click the Ethernet interface that you require:

- Local Area Connection
- Local Area Connection 2

Step 3 Change the Interface Type to "Private interface connected to private network" from "Public interface connected to the Internet".

Step 4 Open the CLI and at the command prompt, run **netsh winsock reset**.

Step 5 Restart the machine.

About Cisco Unified Presence Release 7.0(4)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 7.0(4).

- Outlook Presence Gateway Page Does Not Update, page 38
- Verify SIP-TLS Conversion Parameter is Enabled for Federation Integration, page 38
- Meeting Notification is Not Working in Cisco IP Phone Messenger, page 39
- Creating a Custom Certificate for Access Edge Using an Enterprise Certificate Authority, page 39
- Update to Configuring the Certificate on Cisco Adaptive Security Appliance using Manual Enrollment, page 41

Outlook Presence Gateway Page Does Not Update

When configuring the Outlook Presence Gateway, you can use the Certificate Viewer to configure the certificate chain required for a successful Exchange SSL Connection. The Certificate Viewer allows you to accept and save the displayed certificate chain. After you have finished using the Certificate Viewer, close it, and the Outlook Presence Gateway page refreshes to reflect any updates made by the Certificate Viewer.

However, if you have any browser plug-ins that block JavaScript event installed, the actions performed by the Certificate Viewer when it is closed may be blocked. These blocked operations only affect the visual display; all related information is stored correctly on the server. You can verify that the Outlook Presence Gateway information was correctly updated. This update applies to the *Integration Note for Configuring Cisco Unified Presence Release 7.0 with Microsoft Exchange*.

Procedure

Step 1 Sign in to Cisco Unified Presence Administration.

Step 2 Select **Presence > Gateway**s.

Step 3 Select **Find**.

Step 4 Select the Outlook Presence Gateway from the list.

Step 5 Verify that the information is correct.

Verify SIP-TLS Conversion Parameter is Enabled for Federation Integration

If you are using Cisco Unified Presence 7.0(4) within a federated network, you must ensure that the SIP-TLS Conversion to SIP service parameter is enabled. This setting is enabled (On) by default with new installations. Prior to this release the default setting was disabled (Off), which might impact this setting for upgrades. This update applies to the *Integration Guide for Configuring Cisco Unified Presence Release 7.0 for Interdomain Federation*.

Before You Begin

- When you first install Cisco Unified Presence 7.0(4), the SIP-TLS Conversion to SIP parameter is is automatically enabled and set properly for federation.
- If you are upgrading to Cisco Unified Presence 7.0(4) from a previous version, the SIP-TLS Conversion to SIP parameter value retains the previous setting. Because the previous default value was disabled (Off), you should verify this setting and enable it, if necessary.

Procedure

Step 1 Select **Cisco Unified Presence Administration > System > Service Parameters**.

Step 2 Select the Cisco Unified Presence server from the Server menu.

Step 3 Select **Cisco UP SIP Proxy** from the Service menu.

Step 4 Change the **Allow SIP-TLS Conversion to SIP** parameter (in the SIP Parameters (Clusterwide) section) to **On**.

Step 5 Select **Save**.

Meeting Notification is Not Working in Cisco IP Phone Messenger

If your company uses Microsoft Exchange server, Cisco IP Phone Messenger enables users to receive meeting notifications on their Cisco Unified IP phones. However, if this feature does not work if the user ID has a space character included in it.

This behavior is caused by a Microsoft limitation in which the Microsoft WebDAV does not handle the space in the user ID correctly.

This update applies to the *User Guide for Cisco IP Phone Messenger and Cisco Unified Presence Release 7.0*.

Creating a Custom Certificate for Access Edge Using an Enterprise Certificate Authority

Refer to these instructions if you are using a Microsoft Enterprise Certificate Authority to issue a client/server role certificate to the external interface of Access Edge or to the public interface of the Cisco Adaptive Security Appliance.

This update applies to the *Integration Guide for Configuring Cisco Unified Presence Release 7.0 for Interdomain Federation*.

Before You Begin

These steps require that the Certificate Authority is an Enterprise CA and is installed on the Enterprise Edition of either Windows Server 2003 or 2008.

For additional details about these steps, refer to the Microsoft instructions: http://technet.microsoft.com/en-us/library/bb694035.aspx

Creating and Issuing a Custom Certificate Template

Procedure

Step 1 Follow Steps 1- 6 from the Microsoft site: *Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority.*

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

Tip For Step 5, use a more appropriate name for this specific template, such as Mutual Authentication Certificate.

Step 2 Follow these steps in place of Steps 7-12 from the Microsoft site:

a. Select the **Extensions** tab. Make sure that under **Application Policies** that both **Client Authentication** and **Server Authentication** are present and that no other Policies are present. If these policies are not available, then you must add them before proceeding.

   - In the **Edit Application Policies Extension** dialog box, select **Add**.
   - In the **Add Application Policy** dialog box, select **Client Authentication**, press Shift and select **Server Authentication**, and then click **Add**.

  - In the **Edit Application Policies Extension** dialog box, select any other policy that may be present and then select **Remove**.

    In the **Properties of New Template** dialog box, you should now see listed as the description of Application Policies: Client Authentication, Server Authentication.

b. Select the **Issuance Requirement** tab. If you do not want the Certificate to be automatically issued, then select **CA certificate manager approval**. Otherwise, leave this option blank.

c. Select the **Security** tab and ensure that all required users and groups have both read and enroll permission.

d. Select the **Request Handling** tab and select the CSP button.

e. On the **CSP Selection** dialog box select **Requests must use one of the following CSP's**.

f. From the list of CSP's select **Microsoft Basic Cryptographic Provider v1.0 and Microsoft Enhanced Cryptographic Provider v1.0**, and select **OK**.

Step 3 Continue with Steps 13-15 from the Microsoft site: *Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority.*

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

Requesting the Site Server Signing Certificate

Procedure

Step 1 Follow Steps 1-6 from the Microsoft site: *Site Server Signing Certificate for the Server That Will Run the Configuration Manager 2007 Site Server.*

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver2

Tip For Step 5, select the name of the certificate template you created previously, such as Mutual Authentication Certificate and enter the external FQDN of the access edge in the **Name** field.

Step 2 Follow these steps in place of Steps 7-8 from the Microsoft site:

a. If the certificate request is automatically issued then you will be presented with an option to install the signed certificate. Select **Install this Certificate**.

b. If the certificate request is not automatically issued then you will need to wait for the administrator to issue the certificate. Once issued:

  - On the member server, load Internet Explorer and connect to the Web enrollment service with the address http://<*server*>/**certsrv** where <*server*> is the name or IP address of the Enterprise CA.
  - On the Welcome page, select **View the status of a pending certificate request**.

c. Select the issued certificate and select **Install this Certificate**.

Update to Configuring the Certificate on Cisco Adaptive Security Appliance using Manual Enrollment

This update applies to the *Integration Guide for Configuring Cisco Unified Presence Release 7.0 for Interdomain Federation*.

Procedure

Step 1 Enter this sequence of commands to generate a trustpoint to identify the CA:

```
crypto ca trustpoint <name of trustpoint>
fqdn <fqdn_public_cup_address>
client-types ssl
keypair public_key_for_ca
```

Note
- The FQDN value must be the FQDN of the public Cisco Unified Presence address.
- The keypair value must be the keypair created for the CA.

Step 2 Enter this command to configure the enrollment method for the trustpoint:

```
enrollment terminal
```

Step 3 Enter this command to authenticate the certificate:

```
crypto ca authenticate <trustpoint_name>
```

Step 4 Copy and paste the certificate into the terminal.

Step 5 Enter yes when you are prompted to accept the certificate.

Step 6 Enter this command to send an enrollment request to the CA:

```
crypto ca enroll <trustpoint_name>
```

Step 7 For each request generated by the **crypto ca enroll** command, obtain a certificate from the CA for the applicable trustpoint. The certificate should be in base-64 format.

Note If you are using an Enterprise Certificate Authority, select a Certificate Template that provides both Client and Server Authentication. If you are not sure which Certificate Template to use, contact the administrator of the Certificate Authority.

Step 8 Use the **crypto ca import** command to import each certificate you receive from the CA.

Step 9 Paste the base-64 certificate into the terminal.

```
crypto ca import certificate

hostname (config)# crypto ca <trustpoint_name> import certificate
% The fully-qualified domain name in the certificate will be:
<fqdn>
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
hostname (config)#
```

About Cisco Unified Presence Release 7.0(5)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 7.0(5).

- Call Forwarding Status Not Updated on Microsoft Office Communicator Interface, page 42
- Errors Encountered when Upgrading from Cisco Unified Presence Release 1.0(3) to Cisco Unified Presence Release 7.0(5), page 42
- Privacy Policy Pages on Cisco Unified Presence User UI Displays English Phrases in non-English Locale, page 43
- NTP is Not Configurable, page 43
- Cisco Unified Communications Manager Locale Installer for Cisco Unified Presence Release 7.0(5), page 43
- Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 7.0(5) Fail with a Sign Error, page 43
- Inconsistent Behavior with Cisco Unified Presence Evaluation License, page 43

Call Forwarding Status Not Updated on Microsoft Office Communicator Interface

Cisco Unified Presence allows enterprise users to control their Cisco Unified IP Phone through Microsoft Office Communicator. In this deployment, if a user turns on or turns off the Call Forwarding feature from the Microsoft Office Communicator interface, the status of the Call Forwarding feature is updated on the Cisco Unified IP Phone of the user. However, if a user turns on or turns off the Call Forwarding feature from their Cisco Unified IP Phone, the status of the Call Forwarding feature is *not* updated on the Microsoft Office Communicator interface of the user.

Errors Encountered when Upgrading from Cisco Unified Presence Release 1.0(3) to Cisco Unified Presence Release 7.0(5)

Problem

When upgrading from Release 1.0(3) to Release 7.0(5) in Cisco Unified OS Administration, the upgrade window returns errors.

Cause

This condition occurs when you are using Cisco Unified OS Administration (**Software Upgrades > Install/Upgrade**) to upgrade from Release 1.0(3) to Release 7.0(5) of Cisco Unified Presence.

Solution

We recommend that you upgrade from Release 1.0(3) to a pre-7.0(5) release of Cisco Unified Presence, for example, Release 7.0(4). Then upgrade Cisco Unified Presence again to Release 7.0(5).

Privacy Policy Pages on Cisco Unified Presence User UI Displays English Phrases in non-English Locale

Problem

The Privacy Policy pages on the Cisco Unified Presence user UI display some phrases in English only. This means that even if a non-English locale has been installed, the user UI will still display some phrases in English.

Cause

This condition occurs only on the Cisco Unified Presence User UI (Privacy Policy pages) when a non-English locale has been installed (and selected) by a user.

Solution

No workaround exists. English is the only locale supported on the Privacy Policy pages in the Cisco Unified Presence User Options Interface.

NTP is Not Configurable

By design, NTP is not configurable on Cisco Unified Presence Release 7.0(5).

Related Topics

Documentation Changes, page 61

Cisco Unified Communications Manager Locale Installer for Cisco Unified Presence Release 7.0(5)

Cisco Unified Communications Locale Installer 7.0.4.1000 is the latest locale installer for Release 7.0(5) of Cisco Unified Presence.

Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 7.0(5) Fail with a Sign Error

For more information, see Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3.

Inconsistent Behavior with Cisco Unified Presence Evaluation License

Problem

After a fresh installation of Cisco Unified Presence, the system defaults to Evaluation mode for 90 days. If, during this trial period, you use an Evaluation license to access Cisco Unified Presence Release 7.0(5) or a higher release, the following inconsistent behavior may occur:

- The Cisco Unified Presence Administration interface will show all users to be licensed for Cisco Unified Presence and Cisco Unified Personal Communicator even if those users do not have the license capability assigned in Cisco Unified Communication Manager.
- As a result, a user will be able to authenticate and connect to Cisco Unified Presence for Instant Message (IM) and presence capabilities. However, Cisco Unified Communication Manager will not publish phone presence requests unless those users are licensed from Cisco Unified Communication Manager.

Cause

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

Solution

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

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

About Cisco Unified Presence Release 7.0(6)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 7.0(6).

- Device Partition Information Does Not Display in MOC-RCC Drop-Down List, page 44
- Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 7.0(6) Fail with a Sign Error, page 44

Device Partition Information Does Not Display in MOC-RCC Drop-Down List

Problem

If the user has the same Directory Number (DN) in two different partitions, information about the device partitions are not visible in the phone selection menu on the Phone Selection plug-in for the Microsoft Office Call Control feature.

Cause

This condition occurs when the you configure the same DN in multiple partitions

Solution

No workaround exists.

Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 7.0(6) Fail with a Sign Error

For more information, see Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3.

About Cisco Unified Presence Release 7.0(7)

The following section contains important information for Cisco Unified Presence Release 7.0(7).

- Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 7.0(7) Fail with a Sign Error, page 45

Upgrade from Cisco Unified Presence Releases 1.0(3) and 6.0(1) to Release 7.0(7) Fail with a Sign Error

For more information, see Supported Upgrade Paths to Cisco Unified Presence Release 7.0(x), page 3

About Cisco Unified Presence Release 7.0(8)

The following section contains important information for Cisco Unified Presence Release 7.0(8).

- Slow Response from IDS Database Cause Cisco Unified Personal Communicator Sign In to Fail, page 45
- Exchange Certificate Validation Issue in Cisco Unified Presence Administration, page 45
- Proxy Profile Configuration in Cisco Unified Presence Release 7.0(8), page 46

Slow Response from IDS Database Cause Cisco Unified Personal Communicator Sign In to Fail

Problem

When Cisco Unified Personal Communicator clients attempt to sign in to a backup Cisco Unified Presence server after the primary Cisco Unified Presence server fails, the sign in fails. This issue has been observed during failover and failback testing.

Cause

Slow response times from the IDS database cause this condition to occur.

Solution

No workaround exists.

Exchange Certificate Validation Issue in Cisco Unified Presence Administration

Problem

When you configure a Presence Gateway (Microsoft Outlook - Exchange) in Cisco Unified Presence Administration, the Presence Gateway Configuration window provides a troubleshooter that displays the Exchange server status. In certain circumstances, the *Exchange SSL Connection/Certificate Verification* status can display incorrect information and verify that the connection is fine when it is not.

Cause/ Solution

Cause	Solution
The Exchange SSL Connection/Certificate Verification status will incorrectly indicate that the connection is fine if the security certificate uploaded for this Calendaring feature is a self-signed certificate without CA bit.	You must use a different security certificate for Calendaring. For more information, see the *Integration Node for Configuring Cisco Unified Presence with Microsoft Exchange.*
If you upload security certificates using the Cisco Unified Operating System Administration interface, certain certificates may not upload successfully. This can occur if the certificate that you are uploading contains special characters in the Common Name of the certificate for example, forward slash (/). If, as a workaround, you manually upload such certificates to the Cisco Unified Presence server using a Remote Support Account, the Exchange SSL Connection/Certificate Verification status may incorrectly indicate that the connection is missing required certificates.	You can ignore the incorrect system verification if the Calendaring feature is operating correctly.

Proxy Profile Configuration in Cisco Unified Presence Release 7.0(8)

Proxy profiles are not used and should not be configured with this release of Cisco Unified Presence. The functionality is inaccessible on the Cisco Unified Presence Administration interface. If you upgrade from Cisco Unified Presence Release 6.x to 7.x, we recommend that you delete any proxy profiles that may have been previously configured.

About Cisco Unified Presence Release 7.0(9)

The following section contains important information for Cisco Unified Presence Release 7.0(9).

- Unlocking a User Account on Cisco Unified Presence, page 46

Unlocking a User Account on Cisco Unified Presence

Problem

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

Cause

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

Solution

Procedure

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

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

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

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

Step 5 Select **Save**.

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

Caveats

- Using Bug Toolkit, page 47
- Software Caveats, page 48
- Hardware Caveats, page 48
- Resolved Caveats, page 49

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

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

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

Software Caveats

- IPSec Security Password Mismatch, page 48

IPSec Security Password Mismatch

This section addresses the following defect:

- CSCty38548 GUI can not escape the @ symbol in the IPSec password field on the Cisco Unified Communications Manager 7.x Publisher page.

Problem

When the @ symbol is used in the security password for Cisco Unified Communications Manager Release 7.x, Cisco Unified Presence Release 7.0(9) can not resolve the special character. As a result, Cisco Unified Presence logs an IPSec security password mismatch error.

Solution

Set a password that does not contain the @ symbol.

Hardware Caveats

- HP SCSI Hard Drive Firmware Update, page 48

HP SCSI Hard Drive Firmware Update

This section addresses the following third-party defect:

- CSCse71185 Certain HP Ultra320 SCSI HDs may exhibit reduced performance and timeouts.

Problem

A ProLiant server that is configured internally or externally with any of the HP Ultra320 SCSI hard drives listed at the following page:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00677430

may exhibit reduced performance or have excessive timeouts. This performance issue is caused by the dynamically adjusted seek time profile table in the drive firmware after it becomes degraded.

When this problem occurs, the reduced performance is characterized by occasional brief delays in command response time while servicing random workloads and in severe cases the drive may exhibit command timeouts, which requires a server reboot for recovery.

This problem occurs on the following hard drive models:

- MCS-7835-H1
- MCS-7845-H1

Solution

You may download updated firmware directly from the HP website. Reduced performance and excessive timeouts can be corrected by upgrading the firmware version to:

- HPB5 or later versions for the drives in Table 1 of the HP TechSupport page
- Firmware version HPB9 or later versions for the drives in Table 2 of the HP TechSupport page.

The firmware has been modified to detect and correct invalid seek time profile table values on drives that have already encountered this issue, as well as to eliminate the possibility of subsequent degradation of these same seek-time profile table values. Upgrading the firmware will restore drives already exhibiting this issue to nominal levels of performance, as well as preventing any recurrence of this issue.

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 47).

- Cisco Unified Presence Release 7.0(2), page 49
- Cisco Unified Presence Release 7.0(3), page 50
- Cisco Unified Presence Release 7.0(4), page 52
- Cisco Unified Presence Release 7.0(5), page 53
- Cisco Unified Presence Release 7.0(6), page 54
- Cisco Unified Presence Release 7.0(7), page 54
- Cisco Unified Presence Release 7.0(8), page 55
- Cisco Unified Presence Release 7.0(9), page 56

Cisco Unified Presence Release 7.0(2)

Table 3 lists caveats that are resolved in Cisco Unified Presence Release 7.0(2) but that may have been open in previous releases.

Table 3 Resolved Caveats for Cisco Unified Presence Release 7.0(2)

Identifier	Severity	Component	Headline
CSCso74239	2	config-agent	CA: MER route are comment while sipd is activated
CSCsr63025	3	database	DB: pe and oamagent core from CDBNotifyClientSM
CSCsr88418	3	epe	EPE: PE's CN clients need to be aware of subscription removal
CSCso83160	3	epe	PE lookup of uritoiuid table is case sensitive however OCS ignores case
CSCsr08247	3	epe	Stopping TT service does not always stop PE
CSCsr94203	3	epe	Retry on Refresh Subscription should not contain a suppress-notify-if-ma
CSCsr38466	3	epe	CUP 7.0: if self added to buddy list, status changes to offline
CSCsr93874	3	epe	Federation: SUBSCRIBE after terminating NOTIFY contains Route headers

Table 3 Resolved Caveats for Cisco Unified Presence Release 7.0(2) (continued)

Identifier	Severity	Component	Headline
CSCsu60537	3	epe	EPE: EAL FBA Compliance Enhancement
CSCsr84697	2	esp	Proxy: unable to disable RR for CVP
CSCsr89206	2	esp	Proxy core's after 19 hours of Fed Traffic
CSCsr51855	3	esp	esp: merts should handle requests not addressed to a user
CSCsj07417	3	esp	Presence remains "Available" after n/w disconnect
CSCsr62601	3	esp	Stale CUPC registration can lead to loss of 200 OK response for MESSAGE
CSCsu74449	3	esp	Proxy: Avoid ACK Loop caused by misconfig
CSCsr81708	3	gui	gui: resize browser horizontally-only or veritcally-only doesn't redraw
CSCsu42335	3	gui	Soap TroubleShooter Service Throws Null pointer
CSCsr56389	3	gui	GUI: Different Case Privacy Policy Overwrites Existing Policy
CSCsr44303	3	gui	Federation: GUI Supports Adding Same contact using different case
CSCsk47015	3	gui	Application Listener page needs to limit total num of TCP + TLS connection
CSCso29090	3	serviceability	Improve error message when failing to activate services
CSCsm23706	3	serviceability	Add ttlogin dependency to PE Database Network service
CSCsl18904	3	serviceability	EPASSoap cannot change logging level & user counts
CSCsq76595	3	sync agent	service/sa: SA start not permitted sometimes
CSCsr54150	3	sync agent	Sync Agent prints debug level trace regardless of settings
CSCsm76691	3	vos	security/vos: seeing hostname tomcat filename when regenerated
CSCsr51126	3	vos	Deleted Default TLS context will fail upgrade

Cisco Unified Presence Release 7.0(3)

Table 4 lists caveats that are resolved in Cisco Unified Presence Release 7.0(3) but that may have been open in previous releases.

Table 4 Resolved Caveats for Cisco Unified Presence Release 7.0(3)

Identifier	Severity	Component	Headline
CSCsr94201	3	config-agent	EspConfigAgent Core on Shutdown on Inactive Partition over L2
CSCsu36091	2	ctigw	Static Analysis fix for ctigw module
CSCsu30320	2	ctigw	Core in ctigw
CSCsx07942	3	ctigw	CTIGW: QBE Library on CUPS needs to use unmodifiedcgpn
CSCsw14321	3	ctigw	CCM Cti Failover/Fail Back Back Does Not Seem To Work with RCC Control
CSCsv95957	3	ctigw	CTI call tranfer request relayed by CUPS from MOC to CUCM co
CSCsv78069	3	ctigw	MOC not open window for incoming call when Auto Call Pickup is Enabled
CSCsu99420	2	database	CTIGW: phone-context string is hard-coded to dialstring
CSCsr69113	2	database	DB: L2 upgrade failed at cm-dbl-install
CSCsu98667	2	database	Sync Conflicts on typefieldinfo.csv

Table 4 Resolved Caveats for Cisco Unified Presence Release 7.0(3) (continued)

Identifier	Severity	Component	Headline
CSCsv00855	2	database	Build hangs while processing typeruleinfo.csv
CSCsv01805	2	database	Sync Issues on servMMgdWebApp.c
CSCsv37525	3	database	Porting CSCsu80901
CSCsv18985	3	database	method/event routes are misconfigured
CSCsr13083	3	database	N-Node API must support Active/Standby for User Move operations
CSCsq12986	3	database	db/install: subscriber fresh install failure SQLException
CSCsu88195	3	database	peuniqueid_seq not found error when node name is IP instead of hostname
CSCsu43379	3	database	Mail ID change does not update PEResourceProfile automatically
CSCsr81529	3	database	Federation: Presence Lost Upon 2 Way Blocking Configuration Change
CSCsr75615	3	database	softphone flag in CUP DB should reflect actual exsistence of UPC device
CSCsq81834	3	database	Invalid index in add-group message gives generic error message
CSCsx59452	3	database	MOC Phone selection Plugin won't display devices when Multiple EM login
CSCsv05548	2	epe	epe: PE deadlock
CSCsx15113	3	epe	pe core after L2 from 7.0(4) to 7.0(4)
CSCsv00031	3	epe	EPE: can't start pe due to mis-config pe_cfg.xml
CSCsu97394	3	epe	EPE: Utilizing multiple TCP listener ports in contact headers
CSCsu74682	3	epe	EPE:200 OK for cisco-fetch doesn't have ContentType and Require headers
CSCsv56137	3	epe	PE must log when 1 of output bound proxies fails
CSCsv04359	3	epe	EPE: Connection to exchange server lost during CUPC SC/IM load
CSCsr14313	3	epe	CUP: TT: Info:Error in exec statement rc:SQL_ERROR
CSCsu38237	3	esp	Proxy Static Analysis
CSCsu69963	3	esp	Proxy: During failover long ACE timeout to old server causes problems
CSCsv52431	3	esp	CUPS CTI Gw intermittent heartbeat timeouts, interrupting MOC connection
CSCsv10149	3	esp	ESP: proxy cored while removing ICT
CSCsu05502	3	esp	ESP: backend subscription lost on TLS inter-cluster testing
CSCsr07173	3	fed-ocs	Use Mail ID as Contact ID instead of User ID
CSCsr13082	3	gui	Need UserAssignment Mode SP to support Active / StandBy
CSCsr44631	3	gui	gui: presence viewer shows incorrect login status on other nodes
CSCsq84827	3	gui	security: when IC switched to TLS saw Exception: Signature does not match
CSCsq41402	3	gui	CUP: Exception initializing page context java.lang.IllegalStateException
CSCsl70531	3	gui	Web GUI Exception When Adding Incoming ACL After Federated Domain
CSCsx59531	3	gui	MOC Phone selection Plugin should display Device name when logged in EM
CSCsw14345	3	intercluster	GUI duplicate user search causes Java null-pointer exception
CSCsu38455	3	intercluster	CUPInterclusterSyncAgentDuplicateUser alarm should not be critical level
CSCsq81650	3	intercluster	ICSA allows addition of peer which refers to own cluster
CSCsv97810	3	ippm	Cannot login to IP Phone Messenger service if user id has space char

Table 4 Resolved Caveats for Cisco Unified Presence Release 7.0(3) (continued)

Identifier	Severity	Component	Headline
CSCsl04891	3	ippm	IPPM XML Parse error on Deskphone if already logged into IPPM on 7921
CSCsr96028	3	security	ICSA certificate exchange doesn't support intermediate CA transfer
CSCsr65728	3	security	TLS Peer Subject settings for intercluster peers change after L2 upgrade
CSCsr48752	3	security	CUPS upgrade didn't carry PE-trust certs over in Tomcat directory
CSCsu01756	2	serviceability	Cisco UP Presence Engine Database service not correct in SYSAPPL-MIB
CSCsu01913	3	soap-interface	Client Config Interface in compatible with Axis 2 - 1.4
CSCsr32177	3	soap-interface	XML reserved characters in privacy policy name cause CUPC login failure
CSCsv49536	2	vos	Memory Leak related to code associated with changing IPSecMasterHost
CSCsu38376	3	vos	vos/install: strict pw check isn't in unattended,VM, pre-install servers
CSCsv05264	3	vos	Proxy: empty response code during timeout
CSCsu02332	3	vos	JAVA: java process memory leak on IBM server
CSCsr25733	3	vos	drs: invalid sftp server hangs the drs gui
CSCsr32088	3	vos	vos: after pwrecovery security reset, reboot, old sec pw comes up

Cisco Unified Presence Release 7.0(4)

Table 5 lists caveats that are resolved in Cisco Unified Presence Release 7.0(4) but that may have been open in previous releases.

Table 5 Resolved Caveats for Cisco Unified Presence Release 7.0(4)

Identifier	Severity	Component	Headline
CSCsr97144	2	config-agent	CA depends on isActive
CSCsx44323	3	ctigw	MOC: sipd core ctigw_csta_handler when MOC logs in
CSCsx50660	2	database	L2 Upgrade fails due to misconfigured mail id field in CUCM
CSCsv18985	3	database	method/event routes are misconfigured
CSCsw78962	3	database	Failed to enable calendar in user option
CSCsx03405	6	database	Add company field for LDAP sync
CSCsx15113	3	epe	pe core after L2 from 7.0(4) to 7.0(4)
CSCse60410	3	gui	ST: Unable to display all available CTI Gateway Profiles in CUPS Admin
CSCsr25527	3	gui	CUP:MLA: Can not assign end users to Roles on Cup
CSCsr41343	3	gui	gui: Presence Viewer: user in mixed lower/upper case returns diff output
CSCsr58740	3	gui	MOC troubleshooter raises false alarm on user login EM
CSCsw92579	3	gui	JPN:No checkbox is available for each ACL entry
CSCsx16048	3	gui	CUP: User Option, "Add New" button in English when phrase is translated
CSCsx23695	3	gui	MLA control of Certificate Viewer pages does not work
CSCsx23729	3	gui	Certificate Viewer generates a blank browser window
CSCsx23729	3	gui	Certificate Viewer generates a blank browser window

Table 5 Resolved Caveats for Cisco Unified Presence Release 7.0(4) (continued)

Identifier	Severity	Component	Headline
CSCsv61299	6	gui	too many restrictions on LDAP “Bind Distinguished Name”
CSCsr64333	3	ippm	Serviceability: RTMT counter for IM
CSCsu01756	2	serviceability	Cisco UP Presence Engine Database service not correct in SYSAPPL-MIB
CSCso13814	3	serviceability	PerfMon counters not available after PE/Proxy service restart
CSCsq27328	3	serviceability	RTMT failed to collect coredump file upon servers cored
CSCsx16045	3	serviceability	CUP Failover: CUPC unable to add contact request after failover
CSCsu27024	3	sync agent	Sync Agent fails to sync from CUCM
CSCsr56071	3	vos	Vos: box hung at stopping iptables after reboot
CSCsu04422	3	vos	NTP Inconsistency between CUP pub and sub
CSCsy87952	3	database	MOC RCC Plugin cannot switch when user logs into multiple EM profiles
CSCsy87953	3	database	MOC RCC displays incorrect DN when a user has a "Logout EM Profile"

Cisco Unified Presence Release 7.0(5)

Table 6 lists caveats that are resolved in Cisco Unified Presence Release 7.0(5) but that may have been open in previous releases.

Table 6 Resolved Caveats for Cisco Unified Presence Release 7.0(5)

Identifier	Severity	Component	Headline
CSCsz12036	3	axl	AXL Counter update error
CSCsy24277	3	config-agent	ESP: proxy not up after activated
CSCsv90274	3	config-agent	CA - hook in TimesTen replication into Registy change manager
CSCsy40591	3	config-agent	CA unnecessarily stops services on the first reboot after upgrade
CSCsy48612	3	config-agent	CA should heartbeat Proxy with config time stamp
CSCsz39577	3	config-agent	CA race condition with proxy on startup
CSCsz05017	3	ctigw	MOC RCC can not control deskphone when call failed
CSCsy41162	2	database	IDS Database failed while system Idle
CSCsy68987	2	database	Assert Failed: No Exception Handler
CSCsw63890	3	database	Contact of duplicate user not resolved when intercluster peer removed
CSCsy08713	3	database	DB: L2 upgrade processing epascontacts table takes about 13H
CSCsy41381	3	database	dbmon doesn't handle unresponsive thread well
CSCsy76763	3	database	DB: should defend against whitespace in remote userid on userid change
CSCsz15074	3	database	NEW: User "mapaule" is not able to add buddies
CSCsy08713	3	database	DB: L2 upgrade processing epascontacts table takes about 13H
CSCsy96207	2	epe	Core dump due to duplicate user
CSCsy12868	3	epe	Fall back from 7.0(3) to earlier version causes PE not to startup
CSCsy90373	3	epe	Need to send TT replication listening port

Table 6 Resolved Caveats for Cisco Unified Presence Release 7.0(5) (continued)

Identifier	Severity	Component	Headline
CSCsz29032	3	epe	EPE: RTMT meeting started and meeting ended counters
CSCsy45481	3	epe	User id that contains "&" shows status as OFFLINE
CSCsz28877	3	esp	Core with EA load due to race where scb modified when ready to deleted
CSCsz29008	3	esp	ESP: RTMT number of sipd idle workers/number of sipd workers
CSCsz45780	3	esp	SIP Proxy Restart Needed When Changing Deskphone Control CTI Address
CSCsw92619	3	gui	Row per Page's dropdown list box is empty on any profile configuration
CSCsz04662	3	gui	CUP GUI does not display logged in users...7.0(4)
CSCsz05516	3	gui	CUPS:ccmuser error message when try to bring up "default" policy
CSCsv38127	3	gui	not able to change CUCM publisher on CUP
CSCsy42651	3	gui	CUP admin GUI: Presence Viewer page does not show correct CUMC status
CSCsz28891	3	gui	Presence viewer- Invalid user shown for userid containing '&'
CSCsz07488	5	gui	unsupported CUPC Proxy Listener options in dropdown
CSCsy00642	3	install	install: 7825-H4 U1 install hangs with no info
CSCsw14366	3	pws	3rd Party Api rejects userid with space
CSCsz44417	4	security	DRS unable to contact Local Agent because of ipsec.pem
CSCsm53768	3	soap-interface	EPAS Soap: End User has international characters
CSCsy87999	3	vos	The CLI "utils diagnose module raid" has been broken

Cisco Unified Presence Release 7.0(6)

Table 7 lists caveats that are resolved in Cisco Unified Presence Release 7.0(6) but that may have been open in previous releases.

Table 7 Resolved Caveats for Cisco Unified Presence Release 7.0(6)

Identifier	Severity	Component	Headline
CSCtc10551	4	epas	NTP not configurable on CUPS
CSCtc25079	4	epas	Presence Viewer wrong presence- contact list contains userid with space
CSCtb83965	3	epe	DND clears when secondary phone unregisters from CUCM

Cisco Unified Presence Release 7.0(7)

Table 8 lists caveats that are resolved in Cisco Unified Presence Release 7.0(7) but that may have been open in previous releases.

Table 8 Resolved Caveats for Cisco Unified Presence Release 7.0(7)

Identifier	Severity	Component	Headline
CSCtd09106	3	axl	size for the hostname should match the size of the field in the database
CSCtd44890	3	config-agent	licensing: from 2 evaluation node to 1 license file, 2nd node active

Table 8 Resolved Caveats for Cisco Unified Presence Release 7.0(7) (continued)

Identifier	Severity	Component	Headline
CSCtc80749	3	cpi-appinstall	Server boot time increases with every reboot & Hdw SNMP fails
CSCsv32209	6	cpi-cert-mgt	Unified OS Browser hangs display certificate with bit key more than 1024
CSCtd92986	3	ctigw	Resuming held call on second shared line puts first active call on hold
CSCtd79102	3	ctigw	OCS RCC fails when device name in lower case
CSCtd69174	3	ctigw	MOC RCC failed when DN is e.164
CSCtd32455	6	ctigw	CTI Gw supresses announcement on IP Phone
CSCsz67330	3	database	New proxy service parameter defaults not applied after L2
CSCtc73077	3	database	Extra peresourceprofile causing exception
CSCtd63206	2	esp	SIP Proxy Coredumps on Notify with Overflow in E164 Address
CSCte50557	3	esp	Underscore in url not supported by sipd
CSCtd81644	3	esp	INVITE fails with 404 due to Federation Webex
CSCtc17595	3	esp	IM across subclusters doesn't work
CSCtc79196	3	ippm	CUPS IPPM should escape at sign in UPN usernames in URLs
CSCtc62839	2	intercluster	Cups Users having Primay extension as IPCC extension prevents login
CSCtd63410	3	oamagent	licensing: from 2 evaluation node to 1 license file, 2nd node active
CSCtb89272	3	oamagent	licensing: Sub PE started w/o SW license after L2 from 7.0.4 to 8.0
CSCtd05791	3	security	IMPORTANT TLS/SSL SECURITY UPDATE
CSCtd82576	3	vos	Port CSCtc80749: Server boot up time increases with every reboot
CSCtd63432	3	vos	Port CSCsv32209 Unified OS - Browser hangs trying display cert 4096-bit

Cisco Unified Presence Release 7.0(8)

Table 9 lists caveats that are resolved in Cisco Unified Presence Release 7.0(8) but that may have been open in previous releases.

Table 9 Resolved Caveats for Cisco Unified Presence Release 7.0(8)

Identifier	Severity	Component	Headline
CSCte68866	3	epe	When client loses network connection,presence watchers do not receive update
CSCte97995	1	esp	Proxy Inter-Cluster routing issue with WebEx requests
CSCtf06198	1	esp	CUP 7.0.7 Proxy incorrectly routing to Subscriber homed users
CSCtd14474	2	esp	SIPD Coredumps due to Possible Stack Corruption During Fuzzing
CSCtf06218	2	esp	WebEx users lose presence on failover
CSCtf81211	2	gui	Remove MS icon and modify existing text
CSCtf17244	3	gui	SIP proxy parameters validation check hangs web page
CSCtf99075	3	gui	Problem with Client Configuration Web Service SOAP set-presence-rules
CSCsy87768	3	sametime	Incorrect call status when the whole c2conf is dropped

Table 9 Resolved Caveats for Cisco Unified Presence Release 7.0(8) (continued)

Identifier	Severity	Component	Headline
CSCtd38698	3	security	CUP SSL Certificate Utilizes Weak Hashing Algorithm
CSCsq54465	4	vos	Log rotate error in syslog

Cisco Unified Presence Release 7.0(9)

Table 10 lists caveats that are resolved in Cisco Unified Presence Release 7.0(9) but that may have been open in previous releases.

Table 10 Resolved Caveats for Cisco Unified Presence Release 7.0(9)

Identifier	Severity	Component	Headline
CSCtc99277	3	cpi-os	Upgrade NTPd used within Cisco UCM
CSCti71023	3	ctigw	Deskphone Placed on Autohold when New Conference is setup
CSCtj28657	3	ctigw	Existing call placed on hold when second call transferred to MOC RCC device
CSCtj00169	3	database	No Presence when upgrade from 6.02 to 7.08 when contact has no buddy
CSCth85409	2	epe	PE Does Not Start After Switch Back From 8.5 to 8.0
CSCtc76658	3	gui	Admin GUI error on "User Management"->"Role" page
CSCth97726	3	soap-interface	Login with any passwd after account lockout is permitted with CUPC7

Documentation Updates

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

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

- Cisco Unified Presence Release 7.0(2), page 56
- Cisco Unified Presence Release 7.0(3), page 57
- Cisco Unified Presence Release 7.0(5), page 59
- Cisco Unified Presence Release 7.0(6), page 61

Cisco Unified Presence Release 7.0(2)

- Configuration and Maintenance Guide for Cisco Unified Presence, page 57
- Deployment Guide for Cisco Unified Presence, page 58

Configuration and Maintenance Guide for Cisco Unified Presence

- Documentation Changes, page 57

Documentation Changes

The following updates are documented in the Configuration and Maintenance Guide for Cisco Unified Presence:

- Integration of mobile users with Cisco Unified Presence via the Cisco Unified Mobility Advantage server and Cisco Unified Mobile Communicator client
- Dispersal of users across a multi-node deployment of Cisco Unified Presence via the Active-Standby feature

Deployment Guide for Cisco Unified Presence

- Documentation Changes, page 57

Documentation Changes

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

- Integration of mobile users with Cisco Unified Presence via the Cisco Unified Mobility Advantage server and Cisco Unified Mobile Communicator client
- Dispersal of users across a multi-node deployment of Cisco Unified Presence via the Active-Standby feature

Cisco Unified Presence Release 7.0(3)

- Configuration and Maintenance Guide for Cisco Unified Presence, page 57
- Deployment Guide for Cisco Unified Presence, page 58
- Installation and Upgrade Guide for Cisco Unified Presence, page 58
- Integration Guide for Configuring Cisco Unified Presence with Microsoft Exchange Server, page 58
- Integration Guide for Configuring Cisco Unified Presence with Microsoft OCS for MOC Call Control, page 58
- User Guide for Cisco IP Phone Messenger and Cisco Unified Presence Release 7.0, page 59
- Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation, page 59

Configuration and Maintenance Guide for Cisco Unified Presence

- Documentation Changes, page 57

Documentation Changes

The following updates are documented in the Configuration and Maintenance Guide for Cisco Unified Presence:

- Configuration of the Cisco WebEx conferencing server on Cisco Unified Presence for integration with Cisco Unified Personal Communicator clients.
- Configuration of certificates for the Presence Exchange Gateway in Cisco Unified Presence Administration.
- Provision for email addresses in interdomain federation.

- Configuration of an Microsoft OCS / LCS server type that allows the end-user to select any phone device that they wish to control via MOC.

Deployment Guide for Cisco Unified Presence

- Documentation Changes, page 57

Documentation Changes

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

- Configuration of a Cisco WebEx conferencing server on Cisco Unified Presence to allow users of Cisco Unified Personal Communicator to launch an unscheduled web conference on a Cisco WebEx server.

Installation and Upgrade Guide for Cisco Unified Presence

- Documentation Changes, page 58

Documentation Changes

The following updates are documented in the Installation and Upgrade Guide for Cisco Unified Presence:

- Eliminated a configuration step - the manual addition (by the Administrator) of Cisco Unified Presence servers on Cisco Unified Communications Manager Application Server list is no longer required. This is now performed automatically by Cisco Unified Presence.

Integration Guide for Configuring Cisco Unified Presence with Microsoft Exchange Server

- Documentation Changes, page 58

Documentation Changes

The following updates are documented in the Integration Guide for Configuring Cisco Unified Presence with Microsoft Exchange Server:

- Configuration of certificates for the Presence Exchange Gateway in Cisco Unified Presence Administration.
- Support for AD 2008 and Windows server 2008.

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

- Documentation Changes, page 58

Documentation Changes

The following updates are documented in the Integration Guide for Configuring Cisco Unified Presence with Microsoft OCS for MOC Call Control:

- Information on how to deploy the Phone Selection plug-in on the Microsoft Office Communicator client interface. The Phone Selection plug-in adds a Cisco Unified Presence GUI tab to the Microsoft Office Communicator client that enables the end user to select a phone device to control.

- Configuration of an Microsoft OCS / LCS server type parameter on Cisco Unified Presence to support the Phone Selection plug-in.
- A workaround for the submission of a certificate request on Windows Certificate Authority 2008.

User Guide for Cisco IP Phone Messenger and Cisco Unified Presence Release 7.0

- Documentation Changes, page 58

Documentation Changes

- Information on how to use the Phone Selection tab for the remote call control feature. The Phone Selection tab Microsoft Office Communicator interface, that allows users to select a phone device to control.

Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation

- Documentation Changes, page 59

Documentation Changes

- Information on how to deploy a Load Balancer in the federated network, located between Cisco Unified Presence and Cisco Adaptive Security Appliance.
- Configuration for using email address for interdomain federation.
- A workaround for the submission of a certificate request on Windows Certificate Authority 2008.

Cisco Unified Presence Release 7.0(5)

- Configuration and Maintenance Guide for Cisco Unified Presence, page 59
- Deployment Guide for Cisco Unified Presence, page 60
- Installation and Upgrade Guide for Cisco Unified Presence, page 60
- Integration Guide for Configuring Cisco Unified Presence with Microsoft Exchange Server, page 60
- Integration Guide for Configuring Cisco Unified Presence with Microsoft OCS for MOC Call Control, page 60
- Integration Guide for Configuring Cisco Unified Presence with Microsoft OCS for Interdomain Federation, page 61
- Cisco Unified Operating System Maintenance Guide for Cisco Unified Presence, page 61

Configuration and Maintenance Guide for Cisco Unified Presence

- Documentation Changes, page 59

Documentation Changes

The following updates are documented in the Configuration and Maintenance Guide for Cisco Unified Presence:

- Updates to support the Evaluation Licensing Mode.

- Viewing number of days before the evaluation license expires in the License Unit Report tool.
- Updates to the System Troubleshooter.

Deployment Guide for Cisco Unified Presence

- Documentation Changes, page 60

Documentation Changes

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

- Desscription of the Evaluation Licensing Mode, including the permissions and restrictions of the running Cisco Unified Presence in Evaluation Mode.
- Recommendations when configuring a Clustering over WAN deployment

Installation and Upgrade Guide for Cisco Unified Presence

- Documentation Changes, page 60

Documentation Changes

The following updates are documented in the Installation and Upgrade Guide for Cisco Unified Presence:

- Updates to support the Evaluation Licensing Mode.

Integration Guide for Configuring Cisco Unified Presence with Microsoft Exchange Server

- Documentation Changes, page 60

Documentation Changes

The following updates are documented in the Integration Guide for Configuring Cisco Unified Presence with Microsoft Exchange Server:

- Updates to support multilingual calendaring integration.

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

- Documentation Changes, page 60

The following updates are documented in the Integration Guide for Configuring Cisco Unified Presence with Microsoft OCS for MOC Call Control:

- Updates to support Microsoft OCS Release 2
- Updates to support Cisco Unified IP Phone RT models

Integration Guide for Configuring Cisco Unified Presence with Microsoft OCS for Interdomain Federation

- Documentation Changes, page 61

Documentation Changes

The following updates are documented in the Integration Guide for Configuring Cisco Unified Presence with Microsoft OCS for Interdomain Federation:

- Updates to support Microsoft OCS Release 2

Cisco Unified Operating System Maintenance Guide for Cisco Unified Presence

- Documentation Changes, page 61

Documentation Changes

This guide is updated on the customer-facing DocWiki at this location to confirm that you cannot configure NTP in release 7.0(5) of Cisco Unified Presence:

http://docwiki.cisco.com/wiki/Cisco_Unified_Presence%2C_Release_7.x_--_Changing_Settings_in_Cisco_Unified_Communications_Operating_System

Cisco Unified Presence Release 7.0(6)

- Configuration and Maintenance Guide for Cisco Unified Presence, page 61

Configuration and Maintenance Guide for Cisco Unified Presence

- Documentation Changes, page 61

Documentation Changes

Updates on the customer-facing DocWiki confirm that:

- Release 7.0(6) of Cisco Unified Presence supports embedded '.' wildcard characters in static routes.

  http://docwiki.cisco.com/wiki/Cisco_Unified_Presence%2C_Release_7.x_--_How_to_Route_Network_Traffic_on_Cisco_Unified_Presence#Configuring_Static_Routes
- You must define a route embed template for any static route pattern that contains embedded wildcards.

  http://docwiki.cisco.com/wiki/Cisco_Unified_Presence%2C_Release_7.x_--_Routing_Network_Traffic_on_Cisco_Unified_Presence#How_to_Configure_Route_Embed_Templates_for_Static_Routes_that_Contain_Wildcards

Obtaining Documentation and Submitting a Service Request

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

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

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