Upgrade Guide for Cisco Unity Connection

Release 7.x
Revised October 23, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number:

Upgrade Guide for Cisco Unity Connection

CONTENTS

Preface

This preface contains the following sections:

Audience and Use

The *Upgrade Guide for Cisco Unity Connection* is intended for system administrators and technicians who handle upgrades and changes to the Cisco Unity Connection system configuration.

The *Upgrade Guide for Cisco Unity Connection* focuses on information and procedures necessary for changing the current configuration of the system—that is the hardware and software arrangements that define what Cisco Unity Connection is and what it does—and for upgrading the Connection software to newer versions. The guide does not include information on changing Cisco Unity Connection data (for example, user templates and call handlers).

Documentation Conventions

Table 1 Conventions in the Upgrade Guide for Cisco Unity Connection

Convention	Description
boldfaced text	Boldfaced text is used for: • Key and button names. (Example: Click **OK**.) • Information that you enter. (Example: Enter **Administrator** in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter **ping <IP address>**.)

Table 1 Conventions in the Upgrade Guide for Cisco Unity Connection (continued)

Convention	Description
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete**.)
> (right angle bracket)	A right angle bracket is used to separate selections that you make on menus. (Example: On the Windows Start menu, click **Settings > Control Panel > Phone and Modem Options**.)

The *Upgrade Guide for Cisco Unity Connection* also uses the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **Means reader be warned. In this situation, you might perform an action that could result in bodily injury.**

(For translations of safety warnings listed in this guide, see *Regulatory Compliance and Safety Information for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/regulatory/compliance/ucwarns.html.)

Cisco Unity Connection Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection*. The document is shipped with Cisco Unity Connection and is available at http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html.

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.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

CHAPTER 1

Upgrading Cisco Unity Connection 7.x to the Shipping 7.x Version

This chapter contains the following sections:

Task List for Upgrading Connection 7.x Software to the Shipping 7.x Version Without a Connection Cluster

Added May 2009

Do the following tasks to upgrade an existing Connection 7.x server to the shipping 7.x version (no Connection cluster configured).

1. Confirm that you have the software required for the upgrade. For information on downloading the software from Cisco.com, see the "Installation and Upgrade Information" section of the applicable *Release Notes for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
2. *If the Connection server has languages other than English-United States installed, you want to continue using the languages, and you are upgrading from* Connection *7.0(x) to 7.1(x)*: Download the applicable Connection 7.1(x) language files. See the "Downloading Connection 7.x Language Files" section on page 6-3.

Caution If languages other than English-United States are installed and in use on the Connection server, you must install the Connection 7.1(x) versions of the same languages later during the upgrade. Otherwise, the Connection conversation will not function properly for all users.

3. See the applicable version of *Release Notes for Cisco Unity Connection* for any additional information on upgrading to the shipping version. In particular, note the items in the "Installation and Upgrade Information" section. Release notes are available at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
4. Back up the server by using the Disaster Recovery System. This backup will not be used to restore data on the Connection 7.x system; we recommend it only so that you can revert to the previous version, if necessary.
5. *If you are upgrading during nonbusiness hours*: Run the CLI command **utils iothrottle disable** to speed up the upgrade.

   In an effort to prevent upgrades from adversely affecting system performance during business hours, the upgrade process is throttled and may take several hours to complete. If you are upgrading during a maintenance window, you can speed up the upgrade by disabling the throttling. This decreases the time required for the upgrade to complete but adversely affects Connection performance. For more information on `utils iothrottle disable`, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Caution You cannot disable throttling while an upgrade is running. If you decide to disable throttling after you start an upgrade, you must stop the upgrade, disable throttling, and restart the upgrade from the beginning.

6. Upgrade the Connection software. See the applicable section:
   - Upgrading Connection Software from a Local DVD (from 7.x), page 1-5
   - Upgrading Connection Software from a Network Location or from a Remote Server (from 7.x), page 1-6
7. Install Connection 7.x languages, if applicable. See the "Installing Connection 7.x Language Files" section on page 6-4.
8. *If you disabled the upgrade throttle in Task 5.*: Run the CLI command **utils iothrottle enable** to re-enable the throttle. For more information on `utils iothrottle enable`, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
9. *If you chose to do a later restart at the end of the software upgrade in Task 6.*: Switch to the upgraded partition. See the "Switching to the Upgraded Version of Connection 7.x Software" section on page 1-7.

   (If you chose to automatically restart at the end of the software upgrade, the switch to the upgraded partition is complete.)

Task List for Upgrading Connection 7.x Software to the Shipping 7.x Version in a Connection Cluster

Added May 2009

As the upgrade software is installed, the publisher and subscriber servers continue answering calls and replication occurs. After the upgrade is complete, you switch the two servers, one at a time, to the upgraded software.

Note the following details about how Connection functions during the switch:

- When you switch the publisher server to the upgraded software, the subscriber server answers all calls, but replication does not occur and messages may not be available.
- When you switch the subscriber server to the upgraded software, the publisher server answers all calls, but replication does not occur and messages may not be available.
- About 15 minutes after both servers are switched to the upgraded software, both servers answer calls, replication resumes, and messages are available.

Note the following considerations about the upgrade process:

- Installing the software upgrade requires approximately two hours for each server, for a total of about four hours.
- Switching to the upgraded software requires a few minutes for each server.
- Messages that are recorded while switching to the upgraded software are not replicated. This means that, depending on the Connection server that is accessed, a user may not be able to retrieve new messages. After the upgrade process is complete, messages are replicated. When replication is complete, all messages are available regardless of which Connection server is accessed.
- MWIs and notifications may not be sent. MWIs and notifications synchronize only after the upgrade process is complete.
- After the upgrade process is complete, the servers require about 15 minutes to renegotiate their server status and to replicate messages.

Do the following tasks to upgrade the publisher and subscriber servers in a Connection 7.x cluster to the shipping 7.x version.

1. Confirm that you have the software required for the upgrade. For information on downloading the software from Cisco.com, see the "Installation and Upgrade Information" section of the applicable *Release Notes for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
2. *If the servers have more than one language installed, you want to continue using multiple languages, and you are upgrading from* Connection *7.0(x) to 7.1(x)*: Download the applicable Connection 7.1(x) language files. See the "Downloading Connection 7.x Language Files" section on page 6-3.

Caution If more than one language is installed and in use on the servers, you must install the Connection 7.1(x) versions of the same languages later during the upgrade. Otherwise, the Connection conversation will not function properly for all users.

3. See the applicable version of *Release Notes for Cisco Unity Connection* for any additional information on upgrading to the shipping version. In particular, note the items in the "Installation and Upgrade Information" section. Release notes are available at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
4. Log on to Cisco Unified Serviceability and confirm that the publisher server has Primary status and that the subscriber server has Secondary status. For instructions, see the "Administering a Cisco Unity Connection Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/cluster_administration/guide/7xcuccagx.html.
5. Back up the publisher server by using the Disaster Recovery System. This backup will not be used to restore data on the Connection 7.x system; we recommend it only so that you can revert to the previous version if necessary.

6. *If you are upgrading during nonbusiness hours*: On the publisher server, run the CLI command **utils iothrottle disable** to speed up the upgrade.

   In an effort to prevent upgrades from adversely affecting system performance during business hours, the upgrade process is throttled and may take several hours to complete. If you are upgrading during a maintenance window, you can speed up the upgrade by disabling the throttling. This decreases the time required for the upgrade to complete but adversely affects Connection performance. For more information on `utils iothrottle disable`, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Caution You cannot disable throttling while an upgrade is running. If you decide to disable throttling after you start an upgrade, you must stop the upgrade, disable throttling, and restart the upgrade from the beginning.

7. Upgrade the Connection software on the publisher server. See the applicable section:
   - Upgrading Connection Software from a Local DVD (from 7.x), page 1-5
   - Upgrading Connection Software from a Network Location or from a Remote Server (from 7.x), page 1-6

   The publisher server continues to answer calls.

Caution Do not restart the publisher server and do not switch to the upgraded software during this task. Otherwise, the Connection cluster will not function correctly.

8. *If you are upgrading during nonbusiness hours*: On the subscriber server, run the CLI command **utils iothrottle disable** to speed up the upgrade.
9. Upgrade the Connection software on the subscriber server. See the applicable section:
   - Upgrading Connection Software from a Local DVD (from 7.x), page 1-5
   - Upgrading Connection Software from a Network Location or from a Remote Server (from 7.x), page 1-6

   The subscriber server continues to answer calls.

Caution Do not restart the subscriber server and do not switch to the upgraded software during this task. Otherwise, the Connection cluster will not function correctly.

10. Install Connection 7.x languages, if applicable. See the "Installing Connection 7.x Language Files" section on page 6-4.

    Install languages on the publisher server first, then on the subscriber server.
11. *If you disabled the upgrade throttle on the publisher server in Task 6.*: Run the CLI command **utils iothrottle enable** to re-enable the throttle. For more information on `utils iothrottle enable`, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
12. Switch to the upgraded software on the publisher server. See the "Switching to the Upgraded Version of Connection 7.x Software" section on page 1-7.
13. *If you disabled the upgrade throttle on the subscriber server in Task 8.*: Run the CLI command **utils iothrottle enable** to re-enable the throttle.

14. Switch to the upgraded software on the subscriber server. See the "Switching to the Upgraded Version of Connection 7.x Software" section on page 1-7.
15. About 15 minutes after you complete Task 14., on the publisher server, confirm that the publisher server has Primary status and that the subscriber server has Secondary status. For instructions, see the "Administering a Cisco Unity Connection Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection Release 7.x*.
16. On the subscriber server, confirm that the publisher server has Primary status and that the subscriber server has Secondary status. For instructions, see the "Administering a Cisco Unity Connection Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection Release 7.x*.

Upgrading Connection Software from a Local DVD (from 7.x)

Added May 2009

To Upgrade Connection Software from a Local DVD

Step 1 Insert the DVD into the disc drive on the Cisco Unity Connection server.

Step 2 Log on to Cisco Unified Operating System Administration.

Step 3 From the Software Upgrades menu, click **Install/Upgrade**.

Step 4 On the Software Installation/Upgrade page, in the Source field, click **DVD/CD**.

Step 5 In the Directory field, enter a forward slash (/).

Step 6 Click **Next**.

Step 7 Select the upgrade version that you want to install, and click **Next**.

Step 8 On the next page, monitor the progress of the upgrade.

If you close your browser during this step, you may see the following message when you try to view the Software Installation/Upgrade page again:

```
Warning: Another session is installing software, click Assume Control to take over
the installation.
```

To continue monitoring the upgrade, click **Assume Control**.

You can also monitor the upgrade by using the Real-Time Monitoring Tool.

Step 9 Select the applicable restart action, depending on the configuration:

No Connection cluster	• To install the upgrade software and automatically restart to the upgraded partition, click **Reboot to Upgraded Partition**. • To install the upgrade and restart to the upgraded partition at a later time, click **Do Not Reboot After Upgrade**.
Connection cluster configured	Click **Do Not Reboot After Upgrade**.

Step 10 Click **Next**.

Step 11 If you selected the Do Not Reboot After Upgrade option in Step 9, click **Finish** when the installation of the upgrade software is complete. The Upgrade Status window displays the Upgrade log.

If you selected the Reboot to Upgrade Partition option, note the following:

- Connection services are stopped.
- Data from the partition where the older version is installed is copied to the partition where the newer version is installed. If changes to the database schema require updates to the format of data, that occurs in this step. Note that messages are stored in a common partition, so they are not copied.
- The Connection server restarts and switches to the newer version.

Note You can check the status of the installation of the upgrade software by using the CLI command `show cuc version`. The installation is complete when the inactive partition has the upgraded software and the active partition has the old software.

Upgrading Connection Software from a Network Location or from a Remote Server (from 7.x)

Added May 2009

To Upgrade Connection Software from a Network Location or from a Remote Server

Step 1 Copy the upgrade file to a directory on an FTP or SFTP server that the Cisco Unity Connection server can access.

Step 2 Log on to Cisco Unified Operating System Administration.

Step 3 From the Software Upgrades menu, click **Install/Upgrade**.

Step 4 On the Software Installation/Upgrade page, in the Source field, click **Remote Filesystem**.

Step 5 In the **Directory** field, enter the path to the directory that contains the upgrade file.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the directory path. (For example, if the upgrade file is in the upgrade directory, you must enter **/upgrade**.)

If the upgrade file is located on a Windows server, you must use the applicable syntax for an FTP or SFTP server such as:

- The path must begin with a forward slash (/) and contain forward slashes throughout instead of backward slashes (\).
- The path must start from the FTP or SFTP root directory on the server and must not include a Windows absolute path, which starts with a drive letter (for example, C:).

Step 6 In the **Server** field, enter the server name or IP address.

Step 7 In the **User Name** field, enter the username that will be used to log on to the remote server.

Step 8 In the **User Password** field, enter the password that will be used to log on to the remote server.

Step 9 In the **Transfer Protocol** field, select the applicable transfer protocol.

Step 10 Click **Next**.

Step 11 Select the upgrade version that you want to install and click **Next**.

Step 12 On the next page, monitor the progress of the upgrade.

If you lose your connection with the remote server or close your browser during this step, you may see the following message when you try to view the Software Installation/Upgrade page again:

Warning: Another session is installing software, click Assume Control to take over the installation.

To continue monitoring the upgrade, click **Assume Control**.

You can also monitor the upgrade by using the Real-Time Monitoring Tool.

Step 13 Select the applicable restart action, depending on the configuration:

No Connection cluster	• To install the upgrade software and automatically restart to the upgraded partition, click **Reboot to Upgraded Partition**. • To install the upgrade and restart to the upgraded partition at a later time, click **Do Not Reboot After Upgrade**.
Connection cluster configured	Click **Do Not Reboot After Upgrade**.

Step 14 Click **Next**.

Step 15 If you selected the Do Not Reboot After Upgrade option in Step 13, click **Finish** when the installation of the upgrade software is complete. The Upgrade Status window displays the Upgrade log.

If you selected the Reboot to Upgrade Partition option, not the following:

- Connection services are stopped.
- Data from the partition where the older version is installed is copied to the partition where the newer version is installed. If changes to the database schema require updates to the format of data, that occurs in this step. Note that messages are stored in a common partition, so they are not copied.
- The Connection server restarts and switches to the newer version.

Note You can check the status of the installation of the upgrade software by using the CLI command `show cuc version`. The installation is complete when the inactive partition has the upgraded software and the active partition has the old software.

Switching to the Upgraded Version of Connection 7.x Software

Added May 2009

If you chose not to automatically switch to the upgraded partition at the end of the upgrade, do the following procedure when you are ready to switch partitions.

To Switch to the Upgraded Version of Connection 7.x Software

Step 1 Log on to Cisco Unified Operating System Administration.

Step 2 From the Settings menu, click **Version**.

Step 3 On the Version Settings page, click **Switch Versions**, and the following occurs:

- Connection services are stopped.

- Data from the partition where the older version is installed is copied to the partition where the newer version is installed. If changes to the database schema require updates to the format of data, that occurs in this step. Note that messages are stored in a common partition, so they are not copied.
- The Connection server restarts and switches to the newer version.

Note You can check the status of the installation of the upgrade software by using the CLI command `show cuc version`. The upgrade is complete when the inactive partition has the upgraded software and the active partition has the old software.

CHAPTER 2

Upgrading Cisco Unity Connection 2.x to the Shipping 7.x Version

This chapter contains the following sections:

Task List for Upgrading Connection 2.x Software to the Shipping 7.x Version

1. If you are upgrading Connection on the current server rather than installing a new server, review the *Cisco Unity Connection Supported Platforms List* to determine whether the server requires replacement hard disks or additional RAM. The document is available at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.
2. Obtain the license files for the upgrade to Connection 7.x. Do not install them now; you do so later in the upgrade process. See the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
3. Confirm that you have the software required for the upgrade. For information on downloading the software from Cisco.com, see the "Installation and Upgrade Information" section of the applicable *Release Notes for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.

4. *If the Connection server has languages other than English-United States installed and you want to continue using the languages*: Download the applicable Connection 7.x language files. See the "Downloading Connection 7.x Language Files" section on page 6-3.

Caution If languages other than English-United States are installed and in use on the Connection server, you must install the Connection 7.x versions of the same languages later during the upgrade. Otherwise, the Connection conversation will not function properly for all users.

5. See the applicable version of *Release Notes for Cisco Unity Connection* for any additional information on upgrading to the shipping version. In particular, note the items in the "Installation and Upgrade Information" section. Release notes are available at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
6. Back up the server by using the Disaster Recovery System. If you are replacing hard disks in the server, this backup will be used to restore Connection 2.x data before you upgrade to Connection 7.x. If you are not replacing hard disks, this backup is just a precaution. We recommend it so that you can revert to Connection 2.x, if necessary.
7. Replace hard disks or add RAM, if applicable. See the "Installing a Memory Upgrade or Replacing Hard Disks (Selected Servers Only)" section on page 2-2.

Caution If you replace hard disks, you must also reinstall Connection 2.x and restore data using the DRS backup that you made in Step 6. Ensure that you have a bootable Connection 2.x installation disk available before you begin this procedure.

8. Upgrade software on the Connection server. See the applicable section:
   - Upgrading Connection Software from a Local DVD (from 2.x), page 2-5
   - Upgrading Connection Software from a Network Location or from a Remote Server (from 2.x), page 2-6
9. Install the license files that you obtained in Task 2. See the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
10. Install Connection 7.x languages, if applicable. See the "Installing Connection 7.x Language Files" section on page 6-4.
11. *If users in Connection 2.x had access to Exchange contacts and calendar information:* Adjust the email addresses in external service accounts for each user. See the "Adjusting Email Addresses in External Service Accounts for Users with Access to Exchange Information" section on page 2-8.

Installing a Memory Upgrade or Replacing Hard Disks (Selected Servers Only)

Revised August 26, 2009

Note If you are upgrading a server that does not require a memory upgrade or a hard-disk replacement, skip this section.

Some servers that are qualified for use with Cisco Unity Connection require:

- A memory upgrade to run Connection 7.x in any configuration.
- A memory upgrade to support a specified number of Connection users when both voice recognition and Digital Networking are configured.
- A hard-disk replacement to support a Connection cluster.

See the applicable server-specific table in the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

Warning **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.** Statement 1

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.** Statement 2

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.** Statement 88

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.** Statement 117

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**
• This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
• When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
• If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.** Statement 1021

Warning **To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

(For translations of the preceding safety warnings, see *Regulatory Compliance and Safety Information for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/regulatory/compliance/ucwarns.html.)

To Install a Memory Upgrade or Replace All Hard Disks (Selected Servers Only)

Step 1 Remove the cover.

Step 2 If you are not installing a memory upgrade, skip to Step 3.

Install the memory modules in the applicable slots or locations, depending on the server model, as documented in the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

Caution If you install new memory modules in the wrong slots, the server and operating system may not recognize that they have been installed, and Cisco Unity Connection performance may suffer.

Step 3 If you are not replacing hard disks, skip to Step 4.

Caution You must remove all existing hard disks and install exactly as many hard disks as you remove, or Cisco Unity Connection installation will fail.

Replace all of the hard disks in the server:

a. If you did not use DRS to back up Connection data in Step 6. of the upgrade task list, do so now.

Caution After you replace the hard disks, you must reinstall Connection 2.x and restore Connection 2.x data before you can upgrade to Connection 7.x.

b. Make note of the current locations of the hard disks in the server, including which hard disk is in which hard disk slot. If the replacement fails and you want to revert to the current configuration, you must put the existing hard disks back into their current locations.

c. Remove the drive trays from the server.

d. Remove the old hard disks from the drive trays.

e. Insert the new hard disks into the drive trays.

f. Reinstall the drive trays in the locations that you made note of in Step b.

g. Reinstall Connection 2.x. See the *Installation Guide for Cisco Unity Connection Release 2.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/2x/installation/guide/2xcucigx.html .

h. Restore Connection 2.x data from the DRS backup.

Step 4 Reattach the cover.

Upgrading Connection Software from a Local DVD (from 2.x)

To Upgrade Connection Software from a Local DVD (from 2.x)

Step 1 Insert the DVD into the disc drive on the Cisco Unity Connection server.

Step 2 Log on to Cisco Unified Operating System Administration.

Step 3 From the Software Upgrades menu, click **Install/Upgrade**.

Step 4 On the Software Installation/Upgrade page, in the Source field, click **DVD/CD**.

Step 5 In the Directory field, enter a forward slash (/).

Step 6 Click **Next**.

Step 7 Select the upgrade version that you want to install, and click **Next**.

Step 8 On the next page, monitor the progress of the upgrade.

If you close your browser during this step, you may see the following message when you try to view the Software Installation/Upgrade page again:

```
Warning: Another session is installing software, click Assume Control to take over
the installation.
```

To continue monitoring the upgrade, click **Assume Control**.

You can also monitor the upgrade by using the Real-Time Monitoring Tool.

Step 9 Select the applicable restart action:

After upgrade, automatically restart to upgraded partition	Click **Reboot to Upgraded Partition**.
After upgrade, restart to upgraded partition at a later time	Click **Do Not Reboot After Upgrade**.

Step 10 Click **Next**.

Step 11 If you selected the **Do Not Reboot After Upgrade** option in Step 9, click **Finish** when the installation of the upgrade software is complete. The Upgrade Status window displays the Upgrade log.

If you selected the **Reboot to Upgrade Partition** option, note the following:

- Connection services are stopped.
- Data from the partition where the older version is installed is copied to the partition where the newer version is installed. If changes to the database schema require updates to the format of data, that occurs in this step. Note that messages are stored in a common partition, so they are not copied.
- The Connection server restarts and switches to the newer version.

Note You can check the status of the installation of the upgrade software by using the CLI command `show cuc version`. The installation is complete when the inactive partition has the upgraded software and the active partition has the old software.

Upgrading Connection Software from a Network Location or from a Remote Server (from 2.x)

To Upgrade Connection Software from a Network Location or from a Remote Server (from 2.x)

Step 1 Copy the upgrade file to a directory on an FTP or SFTP server that the Cisco Unity Connection server can access.

Step 2 Log on to Cisco Unified Operating System Administration.

Step 3 From the Software Upgrades menu, click **Install/Upgrade**.

Step 4 On the Software Installation/Upgrade page, in the Source field, click **Remote Filesystem**.

Step 5 In the **Directory** field, enter the path to the directory that contains the upgrade file.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the directory path. (For example, if the upgrade file is in the upgrade directory, you must enter **/upgrade**.)

If the upgrade file is located on a Windows server, you must use the applicable syntax for an FTP or SFTP server such as:

- The path must begin with a forward slash (/) and contain forward slashes throughout instead of backward slashes (\).
- The path must start from the FTP or SFTP root directory on the server and must not include a Windows absolute path, which starts with a drive letter (for example, C:).

Step 6 In the **Server** field, enter the server name or IP address.

Step 7 In the **User Name** field, enter the username that will be used to log on to the remote server.

Step 8 In the **User Password** field, enter the password that will be used to log on to the remote server.

Step 9 In the **Transfer Protocol** field, select the applicable transfer protocol.

Step 10 Click **Next**.

Step 11 Select the upgrade version that you want to install and click **Next**.

Step 12 On the next page, monitor the progress of the upgrade.

If you lose your connection with the remote server or close your browser during this step, you may see the following message when you try to view the Software Installation/Upgrade page again:

```
Warning: Another session is installing software, click Assume Control to take over
the installation.
```

To continue monitoring the upgrade, click **Assume Control**.

You can also monitor the upgrade by using the Real-Time Monitoring Tool.

Step 13 Select the applicable restart action:

After upgrade, automatically restart to upgraded partition	Click **Reboot to Upgraded Partition**.
After upgrade, restart to upgraded partition at a later time	Click **Do Not Reboot After Upgrade**.

Step 14 Click **Next**.

Step 15 If you selected the **Do Not Reboot After Upgrade** option in Step 13, click **Finish** when the installation of the upgrade software is complete. The Upgrade Status window displays the Upgrade log.

If you selected the **Reboot to Upgrade Partition** option, note the following:

- Connection services are stopped.
- Data from the partition where the older version is installed is copied to the partition where the newer version is installed. If changes to the database schema require updates to the format of data, that occurs in this step. Note that messages are stored in a common partition, so they are not copied.
- The Connection server restarts and switches to the newer version.

Note You can check the status of the installation of the upgrade software by using the CLI command `show cuc version`. The installation is complete when the inactive partition has the upgraded software and the active partition has the old software.

Switching to the Upgraded Version of Connection 7.x Software

If you chose not to have Connection automatically switch to the upgraded partition at the end of the upgrade, do the following procedure when you are ready to switch partitions.

To Switch to the Upgraded Version of Connection 7.x Software

Step 1 Log on to Cisco Unified Operating System Administration.

Step 2 From the Settings menu, click **Version**.

Step 3 On the Version Settings page, click **Switch Versions**. The following actions occur:

- Connection services are stopped.
- Data from the partition where the older version is installed is copied to the partition where the newer version is installed. If changes to the database schema require updates to the format of data, that occurs in this step. Note that messages are stored in a common partition, so they are not copied.
- The Connection server restarts and switches to the newer version.

You can check the status of the installation of the upgrade software by using the CLI command `show cuc version`. The installation is complete when the inactive partition has the upgraded software and the active partition has the old software.

Adjusting Email Addresses in External Service Accounts for Users with Access to Exchange Information

The procedure in this section is required for upgrades from Connection 2.x only. (Database entries for external service accounts carry forward in version 7.x.)

With Connection 2.x configured to access Exchange contacts and calendar information, certain features of the Connection 7.x calendar integration may not function correctly (such as sending a voice message to the organizer of or participants in a meeting).

To prevent the problem, do the following procedure in external service accounts for each user who has access to Exchange contacts and calendar information.

To Adjust the Email Address in External Service Accounts for a User with Access to Exchange Information

Step 1 In Cisco Unity Connection Administration, expand **Users**, then click **Users**.

Step 2 On the Search Users page, click the alias of a user.

Step 3 On the Edit User Basics page, from the Edit menu, click **External Service Accounts**.

Step 4 On the External Service Accounts page, click the display name of a service for which the Service Type is Exchange 2007 or Exchange 2003 and the User Access to Calendar is enabled.

Step 5 On the Edit External Service Account page, in the Email Address field, enter the primary SMTP address for the user Exchange mailbox and click **Save**.

Step 6 Click **Test** to verify the entry in the Email Address field.

Step 7 Repeat Step 4 through Step 6 for all remaining services for the user for which the Service Type is Exchange 2007 or Exchange 2003 and the User Access to Calendar is enabled.

Step 8 Repeat this procedure for all remaining users who have access to Exchange contacts and calendar information.

CHAPTER 3

Reverting Servers to the Cisco Unity Connection Version on the Inactive Partition

This chapter contains the following sections:

About Reverting to the Connection Version on the Inactive Partition

Added May 2009

After upgrading, you can revert to the software version that was running before the upgrade by switching to the software version on the inactive partition.

Caution If you revert to the version on the inactive partition, you cannot later switch to the newest version. Instead, you must reinstall the upgrade as documented in this guide.

Caution Do not revert to the version on the inactive partition during regular business hours unless doing so is necessary. Reverting causes the Connection server to restart, and Connection will not function for about 15 minutes, until the restart completes.

Note the following effects on data and messages of reverting to the version on the inactive partition:

- Users that were added after you upgraded to the new version will no longer exist after you revert to the version on the inactive partition. You will have to add the new users again.
- All messages are preserved. However, users that were added after the upgrade no longer exist, so their messages are orphaned. These messages are moved to the undeliverable messages folder.

- If you moved mailboxes from one mailbox store to another after upgrading, those mailboxes will be moved back to the mailbox stores they were in before the upgrade.
- If the version on the inactive partition does not support dispatch messages (any version earlier than Connection 7.0(1)), dispatch messages in the new version of Connection are converted to standard messages in the older version. The subject line still includes "DISPATCH." (Dispatch messages are messages sent to a distribution list, either from a call handler or from an interview handler, that only one user in the group needs to act on. For more information, see the "Dispatch Messages" section in the "Messaging" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.)
- If you revert to Connection 2.x, which does not support future-delivery messages, messages that are queued for future delivery are not deleted from the hard disk, but they will not be delivered, and the sender cannot access them.

Reverting the Servers in a Connection Cluster to the Version on the Inactive Partition

1. Revert the publisher server. See the "Reverting a Connection Server, or the Publisher Server in a Connection Cluster to the Version on the Inactive Partition" section on page 3-2.
2. Revert the subscriber server. See the "Reverting the Subscriber Server in a Connection Cluster to the Version on the Inactive Partition" section on page 3-3.
3. Reset database replication within the cluster. See the "Resetting Database Replication in a Connection Cluster After Reverting the Servers to the Version on the Inactive Partition" section on page 3-3.

Reverting a Connection Server, or the Publisher Server in a Connection Cluster to the Version on the Inactive Partition

To Revert a Connection Server, or the Publisher Server in a Connection Cluster to the Version on the Inactive Partition

Step 1 Log on to Cisco Unified Operating System Administration.

Step 2 From the Settings menu, click **Version**.

The Version Settings window displays.

Step 3 Click the **Switch Versions** button.

After you confirm that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 4 Confirm that the version switch was successful:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **Version**. The Version Settings window displays.

c. Confirm that the correct product version is now running on the active partition.

d. Confirm that all activated services are running.
e. Log on to Cisco Unity Connection Administration.
f. Confirm that the configuration data exists.

Reverting the Subscriber Server in a Connection Cluster to the Version on the Inactive Partition

To Revert the Subscriber Server in a Connection Cluster to the Version on the Inactive Partition

Step 1 Log on to Cisco Unified Operating System Administration.

Step 2 From the Settings menu, click **Version**. The Version Settings window displays.

Step 3 Click the **Switch Versions** button.

After you confirm that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 4 Confirm that the version switch was successful:

a. Log on to Cisco Unified Operating System Administration on the subscriber server.
b. From the Settings menu, click **Version**. The Version Settings window displays.
c. Confirm that the correct version is now running on the active partition.
d. Confirm that all activated services are running.

Resetting Database Replication in a Connection Cluster After Reverting the Servers to the Version on the Inactive Partition

After you revert the servers in a cluster to the version on the inactive partition, you must manually reset database replication within the cluster.

To Reset Database Replication in a Connection Cluster After Reverting the Servers to the Version on the Inactive Partition

On the publisher server, run the CLI command **utils dbreplication reset all**.

CHAPTER 4

Migrating from Cisco Unity Connection 1.x to Version 7.x

This chapter contains the following sections:

About the Tools Used for Migrating Data from Connection 1.x to Version 7.x

Revised May 2009

Note Because Cisco Unity Connection 7.x is installed on a server running Linux instead of Windows, you cannot simply upgrade to version 7.x from version 1.x.

To migrate user data and, optionally, voice messages from a Connection 1.x system to Connection 7.x, you must export the data and messages from the 1.x system by using one of the tools described in the following sections:

- COBRAS (Cisco Objected Backup and Restore Application Suite)
- Connection 1.x to 2.x Migration Export Tool

COBRAS (Cisco Objected Backup and Restore Application Suite)

Advantages of using this tool:

- Exports more data than the Connection 1.x to 2.x Migration Export tool. For more information, see COBRAS Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

- Does not requires a server running a secure shell (SSH) server application.

Disadvantage of using this tool:

- Can export data only from Connection version 1.2.

COBRAS is available at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

Connection 1.x to 2.x Migration Export Tool

Note Updating the Migration Export tool for Connection version 7.x was unnecessary, so although the tool name includes the 2.x version number, the tool functions correctly for a migration export to 7.x.

Advantages of using this tool:

- Can export data from Connection versions 1.1 and 1.2.
- Potentially useful as a backup migration method in case you encounter problems with COBRAS (Cisco Objected Backup and Restore Application Suite).

Disadvantages of using this tool:

- Exports less data than COBRAS. For detailed information on the data that is exported by the Connection 1.x to 2.x Migration Export tool, see Help for the tool at http://www.ciscounitytools.com/HelpFiles/CUC1xTo2xMigrationExport/CUC1xToCUC2xMigrationExport.htm.
- Requires a server running a secure shell (SSH) server application to import Connection 1.x. data and messages. Configuring an SSH server application can be a complicated and time-consuming process. Only OpenSSH for Windows was tested, and customers have reported migration problems when using other SSH applications.

The Migration Export tool is available at http://www.ciscounitytools.com/App_CUC1xTo2xMigrationExport.htm.

Note Exporting Connection data by using the Connection 1.x to 2.x Migration Export tool is not required. However, we recommend this export as a precautionary measure.

Task List for Migrating from Connection 1.x to Version 7.x

Revised May 2009

Use the following high-level task list to migrate to Connection 7.x correctly. The tasks reference detailed instructions in this guide and in other Connection documentation as noted. Follow the documentation for a successful migration.

1. If you are reusing the current Connection server rather than installing a new server, review the *Cisco Unity Connection Supported Platforms List* to determine whether the server requires replacement hard disks or additional RAM. The document is available at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

2. Obtain the license file(s) for the upgrade to Cisco Unity Connection 7.x. Do not install them now; you do so later in the migration process. See the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
3. Review the "Requirements for Migrating from Cisco Unity Connection 1.x to Version 7.x" section of *System Requirements for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html.
4. See the applicable version of *Release Notes for Cisco Unity Connection* for additional information on upgrading to the shipping version. In particular, note the items in the "Installation and Upgrade Information" section. Release notes are available at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
5. Download the following tools:
   - Connection 1.x Disaster Recovery tools, available at http://www.ciscounitytools.com/App_CUC_DisasterRecoveryTool.htm.
   - *For both Connection 1.1 and 1.2:* Connection 1.x to 2.x Migration Export tool, available at http://www.ciscounitytools.com/App_CUC1xTo2xMigrationExport.htm.
   - *If the Connection server is currently running Connection 1.2:* COBRAS, available at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

Note Exporting Connection data by using the Connection 1.x to 2.x Migration Export tool is not required. However, we recommend this export as a precautionary measure.

6. Install the tools that you downloaded in Task 5.
7. Back up the server by using the Connection 1.x Disaster Recovery tools. This backup will not be used to restore data on the Connection 7.x system; we recommend it only so that you can revert to Connection 1.x if necessary.

Note The Connection 1.x Disaster Recovery tools are different from the Disaster Recovery System available with Connection 2.x and later.

8. *If you are exporting from Connection 1.1 and you do not already have a secure shell (SSH) server application installed on a server that is accessible to the Connection 7.x server:* Install one. The migration tool that imports Connection 1.x data into Connection 7.x uses SSH to access the exported user data and messages.
9. Use the Connection 1.x to 2.x Migration Export tool to export Connection 1.x data and messages to the applicable location, depending on the version:

Connection 1.1	Export to the SSH server that is accessible to the Connection 7.x server.
Connection 1.2	If you have a secure shell (SSH) server application installed on a server that is accessible to the Connection 7.x server, export to the SSH server. OR If you do not have an SSH server, you can export data to any network location. You can set up an SSH server later, if necessary. **Note** You use the data exported by the Migration Export tool only if COBRAS fails for some reason when you use it to export data later in the migration process.

See Help for the tool at http://www.ciscounitytools.com/HelpFiles/CUC1xTo2xMigrationExport/CUC1xToCUC2xMigrationExport.htm.

10. *If the Connection server is running version 1.2:* Use COBRAS to export Connection data and messages. For more information, see COBRAS Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.
11. *If additional memory or replacement hard disks are required:* Add memory or replace hard disks. See the "Installing a Memory Upgrade or Replacing Hard Disks (Selected Servers Only)" section on page 4-5 of this guide.
12. Install and begin configuring Connection 7.x. See Part 1 through Part 3 in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html .

13. Populate the system with user and call management data:

Using COBRAS to import	See the following documentation: **a.** The "Importing User Data and Messages by Using COBRAS" section on page 4-9 of this guide. **b.** "Part 4: Populating the System with User and Call Management Data" in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x*. Skip tasks for data that will be imported.
Using Connection 1.x to 2.x Migration Export tool to import	See the following documentation: **a.** Migration Export tool Help. Review for information on data that is exported and imported. **b.** "Part 4: Populating the System with User and Call Management Data" in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x*. Skip tasks for data that will be imported. **c.** The "Preparing to Create User Accounts by Using Multiple Templates" section on page 4-8 of this guide. **d.** The "Importing User Data and Messages by Using the Connection 1.x to 2.x Migration Import Tool" section on page 4-9 of this guide.

14. Finish configuring Connection 7.x. See Part 5 through Part 9 in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x*.

Installing a Memory Upgrade or Replacing Hard Disks (Selected Servers Only)

Note If you are upgrading a server that does not require a memory upgrade or a hard-disk replacement, skip this section.

Some servers that are qualified for use with Cisco Unity Connection require:

- A memory upgrade to run Connection 7.x in any configuration.
- A memory upgrade to support a specified number of Connection users when both voice recognition and Digital Networking are configured.
- A hard-disk replacement to support a Connection cluster.

See the applicable server-specific table in the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

Warning **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.** Statement 1

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.** Statement 2

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.** Statement 88

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.** Statement 117

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**
• This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
• When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
• If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.** Statement 1021

Warning **To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

(For translations of the preceding safety warnings, see *Regulatory Compliance and Safety Information for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/regulatory/compliance/ucwarns.html.)

To Install a Memory Upgrade or Replace Hard Disks (Selected Servers Only)

Step 1 Remove the cover.

Step 2 If you are not installing a memory upgrade, skip to Step 3.

Install the memory modules in the applicable slots or locations, depending on the server model, as documented in the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

Caution If you install new memory modules in the wrong slots, the server and operating system may not recognize that they have been installed, and Cisco Unity Connection performance may suffer.

Step 3 If you are not replacing hard disks, skip to Step 4.

Caution You must remove existing hard disks and install exactly as many hard disks as you remove, or Cisco Unity Connection installation will fail.

Replace the hard disks:

a. Make note of the current locations of the hard disks in the server, including which hard disk is in which hard disk slot. If the replacement fails and you want to revert to the current configuration, you must put the existing hard disks back into their current locations.

b. Remove the drive trays from the server.

c. Remove the old hard disks from the drive trays.

d. Insert the new hard disks into the drive trays.

e. Reinstall the drive trays in the locations that you made note of in Step a.

Step 4 Reattach the cover.

Preparing to Create User Accounts by Using Multiple Templates

The utility that exports user data from Connection 1.x creates one CSV file with data for all users, and the utility that imports this data into Connection 7.x creates all of the new user accounts by using the same template. If you want to create user accounts by using two or more templates, you may want to split the CSV file into one file per template. (Depending on how you want to split users among templates, it might be faster to create all user accounts with the same template and then update user settings individually.)

To Prepare Multiple CSV Files for Creating User Accounts by Using Multiple Templates

Step 1 In the location to which you exported Connection 1.x data, create a subdirectory for each template that you want to use. Give each subdirectory the same name as the corresponding template.

Step 2 Copy the CSV file to each subdirectory. Use the same filename as the original CSV file, or the import will fail.

Step 3 Copy all of the recorded-name WAV files from the location to which you exported Connection 1.x data to each subdirectory that you created in Step 1. Filenames are in the format <user_alias>_VOICE_NAME.wav.

When you import user data from a CSV file, the corresponding recorded-name WAV files are also imported. The import utility looks for these files only in the directory that contains the CSV file from which you are importing.

Step 4 Open the CSV file in each subdirectory, and delete the rows for the users who you do not want to import by using the corresponding template.

For example, if you were editing the CSV file in a SalesStaffTemplate directory, you would delete all of the rows for all of the users who you do not want to create by using the SalesStaffTemplate.

Importing User Data and Messages by Using COBRAS

Added May 2009

For extensive information on importing user data and, optionally, messages into Connection 7.0, see the COBRAS Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

Importing User Data and Messages by Using the Connection 1.x to 2.x Migration Import Tool

If you exported both user data and messages, you must import user data before you import messages.

When you import user data into Cisco Unity Connection 7.x, the Migrate Users utility does not confirm that passwords meet the password requirements specified by Connection credential policies. The first time users log on to Connection 7.x by phone or log on to a web tool, they are prompted to change the password. Credential policies will enforce password requirements. If the user data you import contains any blank passwords, those new user accounts will be created with the default password of the chosen template.

This section contains two procedures, one for importing user data and the other for importing messages.

To Import User Data into a Connection 7.x System

Step 1 In Cisco Unity Connection Administration, expand **Tools**, expand **Migration Utilities**, and click **Migrate Users**.

Step 2 In the **Server Name or IP Address** field, enter the name or the IP address of the SSH server to which you copied Connection 1.x user data.

Step 3 In the **Path Name** field, enter the path to the directory that contains the user data that you want to import.

The format of the path depends on how you configured the SSH server application for access to that directory.

Step 4 In the **User Name** and **Password** fields, enter the account name and password for an account that has the permissions required to access the server and files to which you exported the data.

Step 5 For **User Template**, choose the template whose settings you want to apply to all of the users you are creating with the imported data.

Step 6 In the Failed Objects Filename field, enter the filename for the log file. Connection will save information in the specified file about users whose data could not be imported.

Step 7 Click **Submit**.

When the import is finished, the Status displays “Bulk Administration Tool completed,” as well as the number of users for which the import process succeeded and the number for which it failed.

Step 8 If the import failed for any users, review the file that you specified in Step 6 for information on which user accounts could not be created, and correct the errors as applicable.

You can ignore errors for accounts that are common to all versions of Connection, for example, Operator and UndeliverableMessagesMailbox.

If the import failed for only a few accounts, it may be faster to create the missing accounts manually in Cisco Unity Connection Administration.

Caution If you create accounts manually and you want to import messages that you exported from Connection 1.x, you must give each account the exact alias and SMTP address that the corresponding Connection 1.x account had. If you give the new account a different alias and/or SMTP address, Connection 7.x will not be able to associate the imported messages with the new accounts.

Step 9 Correct user data that could not be imported and reimport it, if applicable:

a. Save the log file locally. This file, which contains only rows for the users who could not be imported, is the file you specified in the Failed Objects Filename field in Step 6.

b. Correct data in the log file.

c. Change the name of the log file to match the name of the CSV file that you imported from, CUCMigrationOutput.csv.

d. Copy the renamed log file into the directory that contains the CSV file that you imported from, and overwrite the original CSV file.

e. Repeat Step 2 through Step 8 until all of the accounts are successfully imported.

Caution If you exported messages as well as user data, you must successfully create all user accounts before you import messages, or the message import will fail.

Step 10 If you created more than one CSV file so that you could import by using more than one template, repeat Step 2 through Step 8 for each of the remaining CSV files that you created in the "To Prepare Multiple CSV Files for Creating User Accounts by Using Multiple Templates" procedure on page 4-8.

To Import Messages into a Connection 7.x System

Step 1 In Cisco Unity Connection Administration, expand **Tools**, expand **Migration Utilities**, and click **Migrate Messages**.

Step 2 In the **Server Name or IP Address** field, enter the name or the IP address of the SSH server to which you exported Connection 1.x user data and messages.

Step 3 In the **Path Name** field, enter the path to the directory that contains the messages that you want to import.

The format of the path depends on how you configured the SSH server application for access to that directory.

Step 4 In the **User Name** and **Password** fields, enter the account name and password for an account that has the permissions required to access the server and files to which you exported the data.

Step 5 Click **Submit**.

When the import is finished, the Status displays "Bulk Administration Tool completed," as well as the number of messages migrated.

CHAPTER 5

Migrating from Cisco Unity 4.x or Later to Cisco Unity Connection 7.x

This chapter contains the following sections:

About the Tools Used for Migrating from Cisco Unity 4.x or Later to Connection 7.x

Revised May 2009

To migrate user data and, optionally, voice messages from a Cisco Unity 4.x or later system to Connection 7.x, you must export the data and messages from the Cisco Unity system by using one of the tools described in the following sections:

- COBRAS (Cisco Objected Backup and Restore Application Suite)
- Cisco Unity 4.x to Connection 2.x Migration Export tool

COBRAS (Cisco Objected Backup and Restore Application Suite)

Advantages of using this tool:

- Exports more data than the Cisco Unity 4.x to Connection 2.x Migration Export tool. For more information, see COBRAS Help at http://www.ciscounitytools.com/Applications/COBRAS/Help/COBRAS.htm.
- Does not require a server running a secure shell (SSH) server application.

Disadvantage of using this tool:

- Can export data only from Cisco Unity 4.0(5) and later.

COBRAS is available at http://www.ciscounitytools.com/App_COBRAS.htm.

Cisco Unity 4.x to Connection 2.x Migration Export tool

Note Updating the Migration Export tool for Connection version 7.x was unnecessary, so although the tool name includes Connection 2.x, the tool functions correctly for a migration export to 7.x. In addition, although the tool name includes only Cisco Unity version 4.x, the tool functions correctly for an export from versions 5.x and 7.x.

Advantages of using this tool:

- Can export data from Cisco Unity versions 4.0(1) through 4.0(4).
- Potentially useful as a backup migration method in case you encounter problems with COBRAS (Cisco Objected Backup and Restore Application Suite).

Disadvantages of using this tool:

- Exports less data than COBRAS. For detailed information on the data that is exported by the Cisco Unity 4.x to Connection 2.x Migration Export tool, see Help for the tool at http://www.ciscounitytools.com/HelpFiles/CUC/CUCMigrationExport/UnityToConnectionMigrationExport.htm.
- Requires a server running a secure shell (SSH) server application to import Cisco Unity 4.x and later data and messages. Configuring an SSH server application can be a complicated and time-consuming process.

The Migration Export tool is available at http://www.ciscounitytools.com/App_CUCMigrationExport.htm.

Note Exporting Cisco Unity data by using the Cisco Unity 4.x to Connection 2.x Migration Export tool is not required for systems running Cisco Unity 4.0(5) or later. However, we recommend this export as a precautionary measure.

Task List for Migrating from Cisco Unity 4.x or Later to Connection 7.x

Revised August 26, 2009

Use the following high-level task list to migrate to Connection 7.x correctly. The tasks reference detailed instructions in this guide and in other Connection documentation as noted. Follow the documentation for a successful migration.

1. If you are reusing the current Cisco Unity server rather than installing a new server, review the *Cisco Unity Connection Supported Platforms List* to determine whether the server requires replacement hard disks or additional RAM. The *Cisco Unity Connection Supported Platforms List* is available at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

2. Obtain Cisco Unity Connection 7.x license file(s). Do not install them now; you do so later in the migration process. See the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Note When you are configuring a Connection cluster, the license that has the MAC address of the publisher server must be installed on the publisher server. The license that has the MAC address of the subscriber server must be installed on the subscriber server.

3. Review the "Requirements for Migrating from Cisco Unity 4.x or Later to Cisco Unity Connection Version 7.x" section in *System Requirements for Cisco Unity Connection 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html.

4. See the applicable version of *Release Notes for Cisco Unity Connection* for additional information on the shipping version of Cisco Unity Connection. In particular, note the items in the section "Installation and Upgrade Information." Release notes are available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/release/notes/701cucrn.html.

5. *Optional but recommended if the Cisco Unity server is running version 4.0(1) through 4.0(4):* Download the software for upgrading to Cisco Unity 4.0(5) or later. For more information, see the section on downloading software in the applicable release notes at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

   COBRAS, the preferred tool because it exports significantly more data from Cisco Unity, works only with Cisco Unity 4.0(5) or later. The potential time savings associated with using COBRAS significantly outweighs the time required to upgrade Cisco Unity.

6. Download the following tools:

   - The Cisco Unity Disaster Recovery tools, available at http://www.ciscounitytools.com/App_DisasterRecoveryTools.htm.
   - If the Cisco Unity server is currently running version 4.0(5) or later or if you will upgrade the server to version 4.0(5) or later during the migration, COBRAS, available at http://www.ciscounitytools.com/App_COBRAS.htm.
   - For Cisco Unity 4.x or later, the Cisco Unity 4.x to Connection 2.x Migration Export tool, http://www.ciscounitytools.com/App_CUCMigrationExport.htm

   Note Exporting Cisco Unity data by using the Cisco Unity 4.x to Connection 2.x Migration Export tool is not required for systems running Cisco Unity 4.0(5) or later. However, we recommend this export as a precautionary measure.

7. Install the tools that you downloaded in Step 6.

8. Back up the server by using the Cisco Unity Disaster Recovery tools. This backup will not be used to restore data on the Connection 7.x system; we recommend it only so you can revert to Cisco Unity if necessary.

9. *If you are using Cisco Unity 4.0(1) through 4.0(4) (the versions that are supported by the Cisco Unity 4.x to Connection 2.x Migration Export tool but are not supported by COBRAS), if you are not upgrading to Cisco Unity 4.0(5) or later so you can use COBRAS, and if you do not already*

have a secure shell (SSH) server application installed on a server that is accessible to the Cisco Unity server: Install an SSH server application. The migration tool that imports Cisco Unity data into Connection 7.x uses SSH to access the exported user data and messages.

Note Only OpenSSH for Windows was tested, and customers have reported problems migrating using other SSH applications.

10. Use the Cisco Unity 4.x to Connection 2.x Migration Export tool to export Cisco Unity data and messages. If the Cisco Unity server is already running Cisco Unity 4.0(5) or later or if you will be upgrading to version 4.0(5) or later during the migration, you will use the data exported by this tool only if COBRAS fails for some reason. For more information, see Help for the tool at http://www.ciscounitytools.com/HelpFiles/CUC/CUCMigrationExport/UnityToConnectionMigrationExport.htm.

    If you have a secure shell (SSH) server application installed on a server that is accessible to the Cisco Unity server, export to the SSH server. If you do not have an SSH server, you can export data to any network location. You can set up an SSH server later if necessary.

11. *Optional but recommended:* If the Cisco Unity server is running version 4.0(1) through 4.0(4), upgrade to Cisco Unity 4.0(5) or later. For more information, see the following documentation:
    - The release notes for the applicable version of Cisco Unity at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.
    - The applicable upgrade chapter in the applicable Reconfiguration and Upgrade Guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

    If the upgrade fails (rare but not impossible), you can either troubleshoot the upgrade or use the data that you exported from Cisco Unity by using the Cisco Unity 4.x to Connection 2.x Migration Export tool.

12. *If the Cisco Unity server is running version 4.0(5) or later:* Use COBRAS to export Cisco Unity data and messages. For more information, see Help for the tool at http://www.ciscounitytools.com/Applications/COBRAS/Help/COBRAS.htm.

13. *If additional memory or replacement hard disks are required:* Add memory or replace hard disks. See the "Installing a Memory Upgrade or Replacing Hard Disks (Selected Servers Only)" section on page 5-5.

14. Install and begin configuring Connection 7.x. See Part 1 through Part 3 in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html .

15. If you exported data and messages by using COBRAS, see the following documentation:
    - The "Importing User Data and Messages by Using COBRAS" section on page 5-8 of this guide.
    - "Part 4: Populating the System with User and Call Management Data" in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x*.

    If you exported data only with the Connection 1.x to 2.x Migration Export tool, see:

- "Part 4: Populating the System with User and Call Management Data" in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x*.
- Preparing to Create User Accounts by Using Multiple Templates, page 5-8
- Importing User Data and Messages by Using the Cisco Unity 4.x to Connection 2.x Migration Export tool, page 5-9

16. Finish configuring Connection 7.x. See Part 5 through Part 9 in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x*.

Installing a Memory Upgrade or Replacing Hard Disks (Selected Servers Only)

Note If you are upgrading a server that does not require a memory upgrade or a hard-disk replacement, skip this section.

Some servers that are qualified for use with Cisco Unity Connection require:

- A memory upgrade to run Connection 7.x in any configuration.
- A memory upgrade to support a specified number of Connection users when both voice recognition and Digital Networking are configured.
- A hard-disk replacement to support a Connection cluster.

See the applicable server-specific table in the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

Warning **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.** Statement 1

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.** Statement 2

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.** Statement 88

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.** Statement 117

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**
• This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
• When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
• If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.** Statement 1021

Warning **To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

(For translations of the preceding safety warnings, see *Regulatory Compliance and Safety Information for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/regulatory/compliance/ucwarns.html.)

To Install a Memory Upgrade or Replace Hard Disks (Selected Servers Only)

Step 1 Remove the cover.

Step 2 If you are not installing a memory upgrade, skip to Step 3.

Install the memory modules in the applicable slots or locations, depending on the server model, as documented in the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

Caution If you install new memory modules in the wrong slots, the server and operating system may not recognize that they have been installed, and Cisco Unity Connection performance may suffer.

Step 3 If you are not replacing hard disks, skip to Step 4.

Caution You must remove existing hard disks and install exactly as many hard disks as you remove, or Cisco Unity Connection installation will fail.

Replace the hard disks:

a. Make note of the current locations of the hard disks in the server, including which hard disk is in which hard disk slot. If the replacement fails and you want to revert to the current configuration, you must put the existing hard disks back into their current locations.

b. Remove the drive trays from the server.

c. Remove the old hard disks from the drive trays.

d. Insert the new hard disks into the drive trays.

e. Reinstall the drive trays in the locations that you made note of in Step a.

Step 4 Reattach the cover.

Preparing to Create User Accounts by Using Multiple Templates

The utility that exports user data from Cisco Unity 4.x creates one CSV file with data for all users, and the utility that imports this data into Connection 7.x creates all of the new user accounts by using the same template. If you want to create user accounts by using two or more templates, you may want to split the CSV file into one file per template. (Depending on how you want to split users among templates, it might be faster to create all user accounts with the same template and then update user settings individually.)

To Prepare Multiple CSV Files for Creating User Accounts by Using Multiple Templates

Step 1 In the location to which you exported Cisco Unity 4.x data, create a subdirectory for each template that you want to use. Give each subdirectory the same name as the corresponding template.

Step 2 Copy the CSV file to each subdirectory. Use the same filename as the original CSV file, or the import will fail.

Step 3 Copy all of the recorded-name WAV files from the location to which you exported Cisco Unity 4.x data to each subdirectory that you created in Step 1. Filenames are in the format <user_alias>_VOICE_NAME.wav.

When you import user data from a CSV file, the corresponding recorded-name WAV files are also imported. The import utility looks for these files only in the directory that contains the CSV file from which you are importing.

Step 4 Open the CSV file in each subdirectory, and delete the rows for the users who you do not want to import by using the corresponding template.

For example, if you were editing the CSV file in a SalesStaffTemplate directory, you would delete all of the rows for all of the users who you do not want to create by using the SalesStaffTemplate.

Importing User Data and Messages by Using COBRAS

Added May 2009

For extensive information on importing user data and, optionally, messages into Connection 7.0, see the COBRAS Help at http://www.ciscounitytools.com/Applications/COBRAS/Help/COBRAS.htm.

Importing User Data and Messages by Using the Cisco Unity 4.x to Connection 2.x Migration Export tool

Note If you exported data by using the COBRAS tool, see COBRAS Help (http://www.ciscounitytools.com/Applications/COBRAS/Help/COBRAS.htm) for information on importing data and messages.

If you exported both user data and messages, you must import user data before you import messages.

Caution Passwords for Cisco Unity web applications cannot be exported because they are stored in Active Directory. When you create new user accounts by importing data, every account will get the same password, which is the password in the template that you specify when you import data.

When you import user data into Cisco Unity Connection 7.x, the Migrate Users utility does not confirm that passwords meet the password requirements specified by Connection credential policies. The first time users log on to Connection 7.x by phone or log on to a web tool, they are prompted to change the password. Credential policies will enforce password requirements. If the user data you import contains any blank passwords, those new user accounts will be created with the default password of the chosen template.

This section contains two procedures, one for importing user data and the other for importing messages.

To Import User Data Into a Connection 7.x System

Step 1 In Cisco Unity Connection Administration, expand **Tools**, expand **Migration Utilities**, and click **Migrate Users**.

Step 2 In the **Server Name or IP Address** field, enter the name or the IP address of the SSH server to which you copied Cisco Unity user data.

Step 3 In the **Path Name** field, enter the path to the directory that contains the user data that you want to import.

The format of the path depends on how you configured the SSH server application for access to that directory.

Step 4 In the **User Name** and **Password** fields, enter the account name and password for an account that has the permissions required to access the server and files to which you exported the data.

Step 5 For **User Template**, choose the template whose settings you want to apply to all of the users you are creating with the imported data.

Step 6 In the Failed Objects Filename field, enter the filename for the log file. Connection will save information in the specified file about users whose data could not be imported.

Step 7 Click **Submit**.

When the import is finished, the Status displays “Bulk Administration Tool completed,” as well as the number of users for which the import process succeeded and the number for which it failed.

Step 8 If the import failed for any users, review the file that you specified in Step 6 for information on which user accounts could not be created, and correct the errors as applicable.

You can ignore errors for accounts that are common to all versions of Connection, for example, Operator and UndeliverableMessagesMailbox.

If the import failed for only a few accounts, it may be faster to create the missing accounts manually in Cisco Unity Connection Administration.

Caution If you create accounts manually and you want to import messages that you exported from Cisco Unity, you must give each account the exact alias and SMTP address that the corresponding Cisco Unity account had. If you give the new account a different alias and/or SMTP address, Connection 7.x will not be able to associate the imported messages with the new accounts.

Step 9 Correct user data that could not be imported and reimport it, if applicable:

a. Save the log file locally. This file, which contains only rows for the users who could not be imported, is the file you specified in the Failed Objects Filename field in Step 6.

b. Correct data in the log file.

c. Change the name of the log file to match the name of the CSV file that you imported from, UnityMigrationOutput.csv.

d. Copy the renamed log file into the directory that contains the CSV file that you imported from, and overwrite the original CSV file.

e. Repeat Step 2 through Step 8 until all of the accounts are successfully imported.

Caution If you exported messages as well as user data, you must successfully create all user accounts before you import messages, or the message import will fail.

Step 10 If you created more than one CSV file so that you could import by using more than one template, repeat Step 2 through Step 8 for each of the remaining CSV files that you created in the "To Prepare Multiple CSV Files for Creating User Accounts by Using Multiple Templates" procedure on page 5-8.

To Import Messages Into a Connection 7.x System

Step 1 In Cisco Unity Connection Administration, expand **Tools**, expand **Migration Utilities**, and click **Migrate Messages**.

Step 2 In the **Server Name or IP Address** field, enter the name or the IP address of the SSH server to which you exported Cisco Unity user data and messages.

Step 3 In the **Path Name** field, enter the path to the directory that contains the messages that you want to import.

The format of the path depends on how you configured the SSH server application for access to that directory.

Step 4 In the **User Name** and **Password** fields, enter the account name and password for an account that has the permissions required to access the server and files to which you exported the data.

Step 5 Click **Submit**.

When the import is finished, the Status displays "Bulk Administration Tool completed," as well as the number of messages migrated.

CHAPTER 6

Adding or Removing Cisco Unity Connection 7.x Languages

This chapter contains the following sections:

Task List for Adding Languages to a Connection 7.x Server Without a Connection Cluster

Revised May 11, 2010

Note Languages are not licensed, and Connection 7.x does not enforce a limit on the number of languages you can install and use. However, the more languages you install, the less hard-disk space is available for storing voice messages. In the *Cisco Unity Connection 7.(x) Supported Platforms List* (http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html), information on the number of minutes of storage available on each server assumes that you have installed no more than five languages.

Do the following tasks to download and install languages in addition to English-United States on a Connection server that is not part of a Connection cluster.

1. Download the Connection languages that you want to install. See the "Downloading Connection 7.x Language Files" section on page 6-3.
2. Install the Connection languages that you downloaded in Task 1. See the "Installing Connection 7.x Language Files" section on page 6-4.

3. *If you are using Japanese because you want Cisco Unity Connection Administration to be localized:* Download and install the Cisco Unified Communications Manager Japanese locale. See the "Locale Installation" section in the "Software Upgrades" chapter of the applicable *Cisco Unified Communications Operating System Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
4. *If you are using additional languages because you want the Cisco Personal Communications Assistant to be localized:* Download and install the corresponding Cisco Unified Communications Manager locales. See the "Locale Installation" section in the "Software Upgrades" chapter of the *Cisco Unified Communications Operating System Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
5. Change language settings in Cisco Unity Connection Administration, as applicable. See the "Changing Connection 7.x Language Settings" section on page 6-6.

Task List for Adding Languages to a Connection 7.x Cluster

Added May 11, 2010

Note Languages are not licensed, and Connection 7.x does not enforce a limit on the number of languages you can install and use. However, the more languages you install, the less hard-disk space is available for storing voice messages. In the *Cisco Unity Connection 7.(x) Supported Platforms List* (http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html), information on the number of minutes of storage available on each server assumes that you have installed no more than five languages.

Do the following tasks to download and install languages in addition to English-United States on both servers in a Connection cluster.

1. Download the Connection languages that you want to install. See the "Downloading Connection 7.x Language Files" section on page 6-3.
2. Change the subscriber server to Primary status (if it does not have Primary status already). The publisher server must have Secondary status in order to install the Connection languages. See the "To Manually Change a Server from Secondary Status to Primary Status" procedure in the "Manually Changing Server Status" section in the "Administering a Cisco Unity Connection Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/cluster_administration/guide/7xcuccagx.html.
3. On the publisher server, install the Connection languages that you downloaded in Task 1. See the "Installing Connection 7.x Language Files" section on page 6-4.
4. *If you are using Japanese because you want Cisco Unity Connection Administration to be localized:* Download and install the Cisco Unified Communications Manager Japanese locale on the publisher server. See the "Locale Installation" section in the "Software Upgrades" chapter of the applicable *Cisco Unified Communications Operating System Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
5. *If you are using additional languages because you want the Cisco Personal Communications Assistant to be localized:* Download and install the corresponding Cisco Unified Communications Manager locales on the publisher server. See the "Locale Installation" section in the "Software Upgrades" chapter of the *Cisco Unified Communications Operating System Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

6. Change the publisher server to Primary status. See the "To Manually Change a Server from Secondary Status to Primary Status" procedure in the "Manually Changing Server Status" section in the "Administering a Cisco Unity Connection Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/cluster_administration/guide/7xcuccagx.html.
7. On the subscriber server, install the same Connection languages that you installed in Task 3.
8. *If you are using Japanese because you want Cisco Unity Connection Administration to be localized:* On the subscriber server, install the Cisco Unified Communications Manager Japanese locale that you installed in Task 4.
9. *If you are using additional languages because you want the Cisco Personal Communications Assistant to be localized:* On the subscriber server, install the same Cisco Unified Communications Manager locales that you installed in Task 5.
10. Change language settings in Cisco Unity Connection Administration, as applicable. See the "Changing Connection 7.x Language Settings" section on page 6-6.

Downloading Connection 7.x Language Files

Added May 2009

To Download Connection 7.x Language Files

Step 1 On a computer with a high-speed Internet connection, go to the Voice and Unified Communications Downloads page at http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875240.

Note To access the software download page, you must be logged on to Cisco.com as a registered user.

Step 2 In the tree control on the Downloads page, expand **Unified Communications Applications > Voicemail and Unified Messaging > Cisco Unity Connection**, and click the applicable Connection version.

Step 3 On the Select a Software Type page, click **Cisco Unity Connection Locale Installer**.

Step 4 On the Select a Release page, click the applicable Connection version. The download links for languages appear on the right side of the page.

Step 5 Confirm that the computer you are using has sufficient hard-disk space for the downloaded files. (The download file sizes appear below the download links.)

The filename for each language is uc-locale-<two-letter language abbreviation>_<two-letter country abbreviation>-<version>.cop.sgn.

Step 6 Click the name of a file to download.

Step 7 On the Download Image page, make note of the MD5 value.

Step 8 Follow the on-screen prompts to complete the download.

Step 9 Repeat Step 6 through Step 8 for each additional Connection language that you want to install.

Step 10 For each downloaded file, use a checksum generator to confirm that the MD5 checksum matches the checksum that is listed on Cisco.com. If the values do not match, the downloaded file is damaged.

Caution Do not attempt to use a damaged file to install software or the results will be unpredictable. If the MD5 values do not match, download the file again until the value for the downloaded file matches the value listed on Cisco.com.

Free checksum tools are available on the Internet—for example, the Microsoft File Checksum Integrity Verifier utility. The utility is described in Microsoft Knowledge Base article 841290, *Availability and Description of the File Checksum Integrity Verifier Utility*. The KB article also includes a link for downloading the utility.

Step 11 Either copy the downloaded files to an FTP or SFTP server, or burn the files to CDs or DVDs. If you burn discs of the files, note the following considerations:

- Use the Joliet file system, which accommodates filenames up to 64 characters long.
- If the disc-burning application that you are using includes an option to verify the contents of the burned disc, choose that option. This causes the application to compare the contents of the burned disc with the source files.
- Label the discs "Cisco Unity Connection <version> Languages."

Step 12 Delete the downloaded files to free disk space.

Installing Connection 7.x Language Files

Added May 2009

You can install language files by using a CD or DVD in the Connection server, or by accessing the files on a remote source. See the applicable section:

- Installing Connection 7.x Language Files from a Disc, page 6-4
- Installing Connection 7.x Language Files from a Network Location or from a Remote Server, page 6-5

Installing Connection 7.x Language Files from a Disc

To Install Connection 7.x Language Files from a Disc

Step 1 Stop the Connection Conversation Manager and Connection Mixer services:

a. Start Cisco Unity Connection Serviceability.

b. From the Tools menu, click **Service Management**.

c. Under Critical Services, in the Connection Conversation Manager row, click **Stop**.

d. Wait for the service to stop.

e. Also under Critical Services, in the Connection Mixer row, click **Stop**.

f. Wait for the service to stop.

Step 2 Insert the Language disc in the disc drive.

Step 3 Log on to Cisco Unified Operating System Administration.

Step 4 From the Software Upgrades menu, click **Install/Upgrade**. The Software Installation/Upgrade window appears.

Step 5 In the Source list, click **DVD/CD**.

Step 6 In the Directory field, enter the path to the folder that contains the language file on the CD or DVD.

If the language file is in the root folder, or if you created an ISO image DVD, enter a slash (/) in the Directory field.

Step 7 To continue the language installation process, click **Next**.

Step 8 Choose the language that you want to install, and click **Next**.

Step 9 Monitor the progress of the download.

Step 10 *If you want to install another language:* Click **Install Another**, and repeat Step 4 through Step 9.

If you are finished installing languages: Restart services:

a. Start Cisco Unity Connection Serviceability.

b. From the Tools menu, click **Service Management**.

c. Under Critical Services, in the Connection Conversation Manager row, click **Start**.

d. Wait for the service to start.

e. Also under Critical Services, in the Connection Mixer row, click **Start**.

f. Wait for the service to start.

g. *If you installed Japanese:* Run the CLI command **utils service restart Cisco Tomcat** to restart the Tomcat service.

Installing Connection 7.x Language Files from a Network Location or from a Remote Server

Revised May 11, 2010

During this procedure, do not use the web browser controls (for example, Refresh/Reload) while accessing Cisco Unified Operating System Administration. Instead, use the navigation controls in the administration interface.

To Install Languages from a Network Location or from a Remote Server

Step 1 Stop the Connection Conversation Manager and Connection Mixer services:

a. Start Cisco Unity Connection Serviceability.

b. From the Tools menu, click **Service Management**.

c. Under Critical Services, in the Connection Conversation Manager row, click **Stop**.

d. Wait for the service to stop.

e. Also under Critical Services, in the Connection Mixer row, click **Stop**.

f. Wait for the service to stop.

Step 2 Log into Cisco Unified Operating System Administration.

Step 3 From the Software Upgrades menu, click **Install/Upgrade**. The Software Installation/Upgrade window displays.

Step 4 In the Source list, click **Remote Filesystem**.

Step 5 In the **Directory** field, enter the path to the folder that contains the language file on the remote system.

If the language file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the folder path. (For example, if the language file is in the languages directory, you must enter **/languages**.)

If the language file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root folder on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

Step 6 In the **Server** field, enter the server name or IP address.

Step 7 In the **User Name** field, enter your username on the remote server.

Step 8 In the **User Password** field, enter your password on the remote server.

Step 9 In the **Transfer Protocol** list, click the applicable option.

Step 10 Click **Next**.

Step 11 Choose the language that you want to install, and click **Next**.

Step 12 Monitor the progress of the download.

If you lose your connection with the server or close your browser during the installation process, you may see the following message when you try to access the Software Upgrades menu again:

Warning: Another session is installing software, click Assume Control to take over the installation.

If you are sure you want to take over the session, click **Assume Control**.

If Assume Control does not display, you can also monitor the language installation with the Real-Time Monitoring Tool.

Step 13 *If you want to install another language:* Click **Install Another**, and repeat Step 3 through Step 12.

If you are finished installing languages, restart services:

a. Start Cisco Unity Connection Serviceability.

b. From the Tools menu, click **Service Management**.

c. Under Critical Services, in the Connection Conversation Manager row, click **Start**.

d. Wait for the service to start.

e. Also under Critical Services, in the Connection Mixer row, click **Start**.

f. Wait for the service to start.

g. *If you installed Japanese:* Run the CLI command **utils service restart Cisco Tomcat** to restart the Tomcat service.

Changing Connection 7.x Language Settings

Added May 2009

Table 6-1 lists the documentation that provides information and procedures for changing language settings.

Table 6-1 Documentation for Changing Language Settings

Language Settings	Documentation
System prompts for all users	The "Language of System Prompts" section in the "Changing Conversation Settings for All Users" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
System prompts for templates, or for one or more individual users	The "Phone Language That Users and Callers Hear" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/user_mac/guide/7xcucmacx.html.
Call handlers	The "Changing Phone Language Settings" section in the "Managing Call Handlers" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x*.
Directory handlers	The "Changing Phone Language Settings" section in the "Managing Directory Handlers" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x*.
Interview handlers	The "Changing Phone Language Settings" section in the "Managing Interview Handlers" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x*.
Call routing tables	The "Changing Phone Language Settings" section in the "Managing Call Routing Tables" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x*.

Removing Connection 7.x Language Files

Added May 11, 2010

To Remove a Connection 7.x Language File

Step 1 Sign in to the command-line interface as a platform administrator.

Step 2 Run the CLI command **show cuc locales** to display a list of installed languages.

Step 3 In the command results, find the language that you want to remove, and note the value of the Locale column for the language.

Step 4 Run the CLI command **delete cuc locale <code>** to remove the language, where <code> is the value of the Locale column that you found in Step 3:

When the command completes, the following information appears:

<code> uninstalled

CHAPTER 7

Replacing Cisco Unity Connection 7.x Servers or Hard Disks

This chapter contains the following sections:

Replacing a Single Connection 7.x Server or the Hard Disks in a Single Server Without a Connection Cluster

Revised March 4, 2010

Use the high-level task list in this section to correctly replace a single Connection 7.x server or to correctly replace the hard disks in a single Connection 7.x server.

Note Do the same tasks if Digital Networking is configured. After data is restored, Digital Networking automatically starts working again.

1. If you are replacing the server, not just replacing the hard disks in the server, order a replacement Connection license that includes the MAC addresses of the replacement server. For details, see the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
2. Use the Disaster Recovery System to back up the Connection server. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

3. Shut down the server.
4. If you are replacing the server, disconnect the network cable from the old server and connect it to the new server.

   If you are replacing hard disks, do the procedure in the "Installing Replacement Hard Disks in a Connection 7.x Server" section on page 7-17.
5. Reinstall Connection. See "Part 1: Installing and Configuring the Cisco Unity Connection Server" in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html .

   When you reinstall Connection, note the following:

   - You must install the same software and ES version that was previously installed on the server, or the Disaster Recovery System restore will fail.
   - You must specify the same hostname and IP address as the previous values, or the Disaster Recovery System restore will fail.
   - Only when you are replacing the server (not when you are replacing only the hard disks), install the replacement license that you ordered in Task 1., which includes the MAC address of the replacement server. Otherwise, Connection will not function.
6. Use the Disaster Recovery System to restore data. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Replacing a Publisher Server or the Hard Disks in a Publisher Server in a Connection 7.x Cluster

Revised March 4, 2010

You can replace the publisher server or replace the hard disks in the publisher server in a Connection cluster without replacing the subscriber server. During the time that the publisher server is not functioning, the subscriber server handles all functions for the Connection cluster to avoid loss of service to the system.

When replacing either the server or the hard disks in the server, you must install a replacement publisher server; you cannot convert the subscriber server into the publisher server. (Replacing hard disks requires that you reinstall all software on the server, so you effectively have a replacement server.) On the replacement publisher server, you configure a new Connection cluster. When you connect the subscriber server to the new Connection cluster, the subscriber server replicates its data to the replacement publisher server without loss of service to the system. When the replacement publisher server has Primary or Secondary status, it begins to handle calls again.

Do the applicable procedures in this section in the order listed.

To Order a Replacement License (Only When You Are Replacing the Publisher Server)

If you are replacing the publisher server, not just replacing hard disks in the publisher server, order a replacement Connection license that includes the MAC address of the replacement server. For details, see the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Disable Digital Networking (Only When Digital Networking Is Configured)

If you are using Digital Networking, disable it by using the procedures in the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Manually Change the Subscriber Server to Primary Status

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, under Server Manager, locate the subscriber server.

Step 4 If the subscriber server has Primary status, skip the remaining steps in this procedure and go to the next procedure.

If the subscriber server has Secondary status, skip to Step 5.

If the subscriber has Deactivated status, change the status to Secondary:

a. In the Change Server Status column for the subscriber server, select **Activate**.

b. When prompted to confirm changing the server status, select **OK**.

c. Confirm that the Server Status column indicates that the subscriber server now has Secondary status.

Step 5 In the Change Server Status column for the subscriber server, select **Make Primary**.

Step 6 When prompted to confirm changing the server status, select **OK**.

The Server Status column displays the changed status when the change is complete.

Note The publisher server will automatically change to Secondary status.

To Manually Change the Publisher Server from Secondary Status to Deactivated Status

Step 1 Sign in to the Real-Time Monitoring Tool (RTMT).

Step 2 On the Cisco Unity Connection menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.

Step 3 In the Node field, select the publisher server.

Step 4 In the right pane, select **Start Polling**.

Step 5 Note whether any voice messaging ports are currently handling calls for the server.

Step 6 Return to the Cluster Management page of Cisco Unity Connection Serviceability.

Step 7 If no voice messaging ports are currently handling calls for the publisher server, skip to Step 8.

If there are voice messaging ports that are currently handling calls for the publisher server, on the Cluster Management page, under Change Port Status, select **Stop Taking Calls** for the publisher server, then wait until RTMT shows that all ports for the publisher server are idle.

Step 8 Under Server Manager, in the Change Server Status column for the publisher server, select **Deactivate**.

Step 9 When prompted to confirm changing the server status, select **OK**.

The Server Status column displays the changed server status when the change is complete.

To Install the Replacement Publisher Server or Hard Disks

Step 1 Shut down the publisher server.

On the subscriber server, in Cisco Unity Connection Serviceability, on the Cluster Management page, the Server Status column shows the publisher server has Not Functioning status.

Step 2 If you are replacing the publisher server, disconnect the network cable from the old publisher server and connect it to the new publisher server.

If you are replacing hard disks, do the procedure in the "Installing Replacement Hard Disks in a Connection 7.x Server" section on page 7-17.

Step 3 Reinstall Connection. Follow the instructions in "Part 1: Installing and Configuring the Cisco Unity Connection Server" in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

When you reinstall Connection, note the following:

- You must install the same software and ES version that is installed on the subscriber server. Otherwise, the Connection cluster may not function correctly.
- You must specify the same hostname as the publisher server that you are replacing. Otherwise, the Connection cluster will not function.
- You must specify the same security password as the publisher server that you are replacing, which also matches the security password for the subscriber server. Otherwise, the Connection cluster will not function. If you do not know the security password, you can change it on the subscriber server before you install the publisher server by using the CLI command **set password user**. For more information, see the applicable version of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
- Only when you are replacing the server (not when you are replacing only the hard disks), install a replacement license that includes the MAC address of the replacement publisher server. Otherwise, Connection will not function.

To Configure the Cluster on the Replacement Publisher Server

Step 1 Sign in to Cisco Unity Connection Administration on the publisher server.

Step 2 In Cisco Unity Connection Administration, expand **System Settings**, then select **Cluster**.

Step 3 On the Find and List Servers page, select **Add New**.

Step 4 On the New Server Configuration page, in the Hostname/IP Address field, enter the hostname or IP address of the subscriber server.

Step 5 In the Description field, enter a description for the subscriber server.

Step 6 Select **Save**.

Step 7 Sign out of Cisco Unity Connection Administration.

To Connect the Subscriber Server to the New Connection Cluster, and Replicate Data and Messages to the Publisher Server

Step 1 Sign in to the command-line interface (CLI) for the subscriber server.

Step 2 Run the CLI command **utils cuc cluster renegotiate**.

Note When the CLI command completes, the publisher server automatically restarts.

Step 3 Run the CLI command **show cuc cluster status** on the subscriber server to confirm that the new Connection cluster has been configured correctly.

To Set Up Digital Networking Again

If you were using Digital Networking before you replaced the publisher server, set it up again by using the procedures in the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Replacing a Subscriber Server or the Hard Disks in a Subscriber Server in a Connection 8.x Cluster

Revised March 4, 2010

You can replace the subscriber server or replace hard disks in the subscriber server in a Connection cluster. During the time that the subscriber server is not functioning, the publisher server will handle all functions for the Connection cluster to avoid loss of service to the system.

When replacing either the server or the hard disks in the server, you remove the subscriber server from the Connection cluster and add the replacement subscriber server. (Replacing hard disks requires that you reinstall all software on the server, so you effectively have a replacement server.) After you install the replacement subscriber server, the publisher server replicates its data to the replacement subscriber server without loss of service to the system. When the replacement subscriber server has Primary or Secondary status, it begins to handle calls again.

Do the applicable procedures in this section in the order listed.

To Order a Replacement License (Only When You Are Replacing the Subscriber Server)

If you are replacing the subscriber server, not just replacing hard disks in the subscriber server, order a replacement Connection license that includes the MAC address of the replacement server. For details, see the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Disable Digital Networking (Only When Digital Networking Is Configured)

If you are using Digital Networking, disable it by using the procedures in the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Manually Change the Publisher Server to Primary Status

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, under Server Manager, locate the publisher server.

Step 4 If the publisher server has Primary status, skip the remaining steps in this procedure and go to the next procedure.

If the publisher server has Secondary status, skip to Step 5.

If the publisher has Deactivated status, change the status to Secondary:

a. In the Change Server Status column for the publisher server, select **Activate**.

b. When prompted to confirm changing the server status, select **OK**.

c. Confirm that the Server Status column indicates that the publisher server now has Secondary status.

Step 5 In the Change Server Status column for the publisher server, select **Make Primary**.

Step 6 When prompted to confirm changing the server status, select **OK**.

The Server Status column displays the changed status when the change is complete.

Note The subscriber server automatically changes to Secondary status.

To Manually Change the Subscriber Server from Secondary Status to Deactivated Status

Step 1 Sign in to the Real-Time Monitoring Tool (RTMT).

Step 2 On the Cisco Unity Connection menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.

Step 3 In the Node field, select the subscriber server.

Step 4 In the right pane, select **Start Polling**.

Step 5 Note whether any voice messaging ports are currently handling calls for the server.

Step 6 Return to the Cluster Management page of Cisco Unity Connection Serviceability.

Step 7 If no voice messaging ports are currently handling calls for the server, skip to Step 8.

If there are voice messaging ports that are currently handling calls for the subscriber server, on the Cluster Management page, under Change Port Status, select **Stop Taking Calls** for the subscriber server, then wait until RTMT shows that all ports for the server are idle.

Step 8 Under Server Manager, in the Change Server Status column for the subscriber server, select **Deactivate**.

Step 9 When prompted to confirm changing server status, select **OK**.

The Server Status column displays the changed server status when the change is complete.

To Install the Replacement Subscriber Server or Hard Disks

Step 1 Shut down the subscriber server.

On the publisher server, in Cisco Unity Connection Serviceability, on the Cluster Management page, the Server Status column shows the subscriber server has Not Functioning status.

Step 2 If you are replacing the subscriber server, disconnect the network cable from the old subscriber server and connect it to the new subscriber server.

If you are replacing hard disks, do the procedure in the "Installing Replacement Hard Disks in a Connection 7.x Server" section on page 7-17.

Step 3 Reinstall Connection. Follow the instructions in "Part 3: Configuring the Cluster, and Installing and Configuring the Subscriber Connection Server" in the "Task List for Installing a Cisco Unity Connection 7.x system with a Connection Cluster Configured" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

When you reinstall Connection, note the following:

- You must install the same software and ES version that is installed on the publisher server. Otherwise, the Connection cluster may not function correctly.

- You must specify the same security password as the subscriber server that you are replacing, which also matches the security password for the publisher server. Otherwise, the Connection cluster will not function. If you do not know the security password, you can change it on the publisher server before you install the subscriber server by using the CLI command **set password user**. For more information, see the applicable version of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
- Only when you are replacing the server (not when you are replacing only the hard disks), you must install a replacement license that includes the MAC address of the replacement subscriber server. Otherwise, Connection will not function.

To Change the Hostname or IP Address for the Subscriber Server in Connection Administration on the Publisher Server (Only If You Changed the Hostname or IP Address of the Subscriber Server)

Step 1 If the replacement subscriber server will have the same hostname or IP address as the subscriber server that you removed, skip the remaining steps in this procedure and go to the next procedure.

If the replacement subscriber server will have a different hostname or IP address, sign in to Cisco Unity Connection Administration on the publisher server.

Step 2 In Cisco Unity Connection Administration, expand **System Settings**, then select **Cluster**.

Step 3 On the Find and List Servers page, select **Find** to display all servers in the cluster.

Step 4 Check the check box in front of the subscriber server and select **Delete Selected**.

Step 5 When prompted to confirm deleting the server, select **OK**.

Step 6 Select **Add New**.

Step 7 On the New Server Configuration page, in the Hostname/IP Address field, enter the hostname or IP address of the replacement server.

Step 8 In the Description field, enter a description for the server.

Step 9 Select **Save**.

Step 10 Sign out of Cisco Unity Connection Administration.

To Confirm That the Connection Cluster Is Configured

Step 1 Sign in to the command-line interface (CLI) for the subscriber server.

Step 2 Run the CLI command **show cuc cluster status**.

To Set Up Digital Networking Again

If you were using Digital Networking before you replaced the subscriber server, set it up again by using the procedures in the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Replacing the Publisher and Subscriber Servers or the Hard Disks in Both Servers in a Connection 7.x Cluster

See the applicable section:

- When Both Original Connection 7.x Servers Are Available and Functioning, page 7-9
- When Neither the of the Original Connection 7.x Servers Is Functioning, page 7-14

When Both Original Connection 7.x Servers Are Available and Functioning

Revised March 4, 2010

When both the publisher and subscriber servers in the Connection cluster are available and functioning, you can replace both servers or replace the hard disks in both servers by completing the process in stages.

- While you are replacing one server, the other server will handle all functions for the Connection cluster to avoid loss of service to the system.
- After each replacement server is installed, the other server replicates data to the replacement server.

Do the applicable procedures in this section in the order listed.

To Order Replacement Licenses (Only When You Are Replacing Servers)

If you are replacing both servers, not just replacing the hard disks in both servers, order replacement Connection licenses that include the MAC addresses of the replacement servers. For details, see the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Disable Digital Networking (Only When Digital Networking Is Configured)

If you are using Digital Networking, disable it by using the procedures in the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Manually Change the Publisher Server to Primary Status

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, under Server Manager, locate the publisher server.

Step 4 If the publisher server has Primary status, skip the remaining steps in this procedure and go to the next procedure.

If the publisher server has Secondary status, skip to Step 5.

If the publisher has Deactivated status, change the status to Secondary:

a. In the Change Server Status column for the publisher server, select **Activate**.

b. When prompted to confirm changing the server status, select **OK**.

c. Confirm that the Server Status column indicates that the publisher server now has Secondary status.

Step 5 In the Change Server Status column for the publisher server, select **Make Primary**.

Step 6 When prompted to confirm changing the server status, select **OK**.

The Server Status column displays the changed status when the change is complete.

Note The subscriber server automatically changes to Secondary status.

To Manually Change a Subscriber Server from Secondary Status to Deactivated Status

Step 1 Sign in to the Real-Time Monitoring Tool (RTMT).

Step 2 On the Cisco Unity Connection menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.

Step 3 In the Node field, select the subscriber server.

Step 4 In the right pane, select **Start Polling**.

Step 5 Note whether any voice messaging ports are currently handling calls for the server.

Step 6 Return to the Cluster Management page of Cisco Unity Connection Serviceability.

Step 7 If no voice messaging ports are currently handling calls for the server, continue to Step 8.

If there are voice messaging ports that are currently handling calls for the subscriber server, on the Cluster Management page, under Change Port Status, select **Stop Taking Calls** for the subscriber server, then wait until RTMT shows that all ports for the server are idle.

Step 8 Under Server Manager, in the Change Server Status column for the subscriber server, select **Deactivate**.

Step 9 When prompted to confirm changing server status, select **OK**.

The Server Status column displays the changed server status when the change is complete.

To Install the Replacement Subscriber Server or Hard Disks

Step 1 Shut down the subscriber server.

On the publisher server, in Cisco Unity Connection Serviceability, on the Cluster Management page, the Server Status column shows the subscriber server has Not Functioning status.

Step 2 If you are replacing the subscriber server, disconnect the network cable from the old subscriber server and connect it to the new subscriber server.

If you are replacing hard disks, do the procedure in the "Installing Replacement Hard Disks in a Connection 7.x Server" section on page 7-17.

Step 3 Install the replacement subscriber server. Follow the instructions in "Part 3: Configuring the Cluster, and Installing and Configuring the Subscriber Connection Server" in the "Task List for Installing a Cisco Unity Connection 7.x system with a Connection Cluster Configured" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

When you reinstall Connection, note the following:

- You must install the same software and ES version that is installed on the publisher server. Otherwise, the Connection cluster may not function correctly.
- You must specify the same security password as the subscriber server that you are replacing, which also matches the security password for the publisher server. Otherwise, the Connection cluster will not function. If you do not know the security password, you can change it on the publisher server before you install the subscriber server by using the CLI command **set password user**. For more information, see the applicable version of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
- Only when you are replacing the server (not when you are replacing only the hard disks), you must install a replacement license that includes the MAC address of the replacement subscriber server. Otherwise, Connection will not function.

To Change the Hostname or IP Address for the Subscriber Server in Connection Administration on the Publisher Server (Only If You Changed the Hostname or IP Address of the Subscriber Server)

Step 1 When you reinstalled Connection, if you specified the same hostname and IP address as those for the subscriber server that you removed, skip this procedure and go to the next procedure.

If the replacement subscriber server has a different hostname or IP address, sign in to Cisco Unity Connection Administration on the publisher server.

Step 2 In Cisco Unity Connection Administration, expand **System Settings**, then select **Cluster**.

Step 3 On the Find and List Servers page, select **Find** to display all servers in the cluster.

Step 4 Check the check box in front of the subscriber server and select **Delete Selected**.

Step 5 When prompted to confirm deleting the server, select **OK**.

Step 6 Select **Add New**.

Step 7 On the New Server Configuration page, in the Hostname/IP Address field, enter the hostname or IP address of the replacement server.

Step 8 In the Description field, enter a description for the server.

Step 9 Select **Save**.

Step 10 Sign out of Connection Administration.

To Confirm That the Connection Cluster Is Configured with the Replacement Subscriber Server

Step 1 Sign in to the command-line interface (CLI) for the subscriber server.

Step 2 Run the CLI command show **cuc cluster status**.

To Manually Change the Subscriber Server to Primary Status

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, select **Cluster Management**.

Step 3 On the Cluster Management page, under Server Manager, locate the subscriber server.

Step 4 If the subscriber server has Primary status, skip the remaining steps in this procedure and go to the next procedure. If the subscriber server has Secondary status, in the Change Server Status column for the subscriber server, select **Make Primary**.

Step 5 When prompted to confirm changing the server status, select **OK**.

The Server Status column displays the changed status when the change is complete.

Note The publisher server will automatically change to Secondary status.

To Manually Change the Publisher Server from Secondary Status to Deactivated Status

Step 1 Sign in to the Real-Time Monitoring Tool (RTMT).

Step 2 On the Cisco Unity Connection menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.

Step 3 In the Node field, select the publisher server.

Step 4 In the right pane, select **Start Polling**.

Step 5 Note whether any voice messaging ports are currently handling calls for the server.

Step 6 Return to the Cluster Management page of Cisco Unity Connection Serviceability.

Step 7 If no voice messaging ports are currently handling calls for the publisher server, skip to Step 8.

If there are voice messaging ports that are currently handling calls for the publisher server, on the Cluster Management page, under Change Port Status, select **Stop Taking Calls** for the publisher server, then wait until RTMT shows that all ports for the publisher server are idle.

Step 8 Under Server Manager, in the Change Server Status column for the publisher server, select **Deactivate**.

Step 9 When prompted to confirm changing the server status, select **OK**.

The Server Status column displays the changed server status when the change is complete.

To Install the Replacement Publisher Server or Hard Disks

Step 1 Shut down the publisher server.

On the Cluster Management page, the Server Status column shows the publisher server has Not Functioning status.

Step 2 If you are replacing the publisher server, disconnect the network cable from the old publisher server and connect it to the new publisher server.

If you are replacing hard disks, do the procedure in the "Installing Replacement Hard Disks in a Connection 7.x Server" section on page 7-17.

Step 3 Reinstall Connection. Follow the instructions in "Part 1: Installing and Configuring the Cisco Unity Connection Server" in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

When you reinstall Connection, note the following:

- You must install the same software and ES version that is installed on the subscriber server. Otherwise, the Connection cluster may not function correctly.
- You must specify the same hostname as the publisher server that you are replacing. Otherwise, the Connection cluster will not function.
- You must specify the same security password as the publisher server that you are replacing, which also matches the security password for the subscriber server. Otherwise, the Connection cluster will not function. If you do not know the security password, you can change it on the subscriber server before you install the publisher server by using the CLI command **set password user**. For more information, see the applicable version of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
- Only when you are replacing the server (not when you are replacing only the hard disks), you must install a replacement license that includes the MAC address of the replacement publisher server. Otherwise, Connection will not function.

To Configure the Cluster on the Replacement Publisher Server

Step 1 Sign in to Cisco Unity Connection Administration on the publisher server.

Step 2 In Cisco Unity Connection Administration, expand **System Settings**, then select **Cluster**.

Step 3 On the Find and List Servers page, select **Add New**.

Step 4 On the New Server Configuration page, in the Hostname/IP Address field, enter the hostname or IP address of the subscriber server.

Step 5 In the Description field, enter a description for the server.

Step 6 Select **Save**.

Step 7 Sign out of Cisco Unity Connection Administration.

To Connect the Subscriber Server to the New Connection Cluster, and Replicate Data and Messages to the Publisher Server

Step 1 Sign in to the command-line interface (CLI) for the subscriber server.

Step 2 Run the CLI command **utils cuc cluster renegotiate**.

Note When the CLI command completes, the publisher server automatically restarts.

Step 3 Run the CLI command **show cuc cluster status** to confirm that the new Connection cluster has been configured correctly.

To Set Up Digital Networking Again

If you were using Digital Networking before you replaced the servers or hard disks, set it up again by using the procedures in the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

When Neither the of the Original Connection 7.x Servers Is Functioning

Revised March 4, 2010

When neither the publisher nor the subscriber server in the Connection cluster is functioning, and when you have a Disaster Recovery System backup from which you can restore the Connection data, you can replace both servers or replace the hard disks in both servers at the same time. During this process, the Connection cluster is not able to answer calls.

You install the replacement publisher server and restore the backed-up Connection data by using Disaster Recovery System. Then you install the replacement subscriber server and force Connection to copy the data from the publisher server to the subscriber server. When the copying is complete, replication will resume between the two servers. When the replacement servers have Primary or Secondary status, they will handle calls.

Do the applicable procedures in this section in the order listed.

To Order Replacement Licenses (Only When You Are Replacing Servers)

If you are replacing both servers, not just replacing hard disks in both servers, order replacement Connection licenses that include the MAC addresses of the replacement servers. For details, see the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Install the Replacement Publisher Server or Hard Disks

Step 1 Shut down the publisher server.

Step 2 If you are replacing the publisher server, disconnect the network cable from the old publisher server and connect it to the new publisher server.

If you are replacing the hard disks, do the procedure in the "Installing Replacement Hard Disks in a Connection 7.x Server" section on page 7-17.

Step 3 Reinstall Connection. Follow the instructions in "Part 1: Installing and Configuring the Cisco Unity Connection Server" in the "Task List for Installing a Cisco Unity Connection 7.x System (Without a Connection Cluster)" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

When you reinstall Connection, note the following:

- You must install the same software and ES version that was installed on the previous publisher server, or the Disaster Recovery System restore will fail.
- You must specify the same hostname and IP address as the values on the previous publisher server, or the Disaster Recovery System restore will fail.
- Only when you are replacing the server (not when you are replacing only the hard disks), you must install a replacement license that includes the MAC address of the replacement publisher server. Otherwise, Connection will not function.

To Restore the Backed-up Data to the Replacement Publisher Server or Hard Disks

Step 1 Sign in to Disaster Recovery System.

Step 2 On the Restore menu, select **Restore Wizard**.

Step 3 On the Step 1 Restore—Choose Backup Device page, in the Device Name field, select the name of the backup device from which you want to restore and select **Next**.

Step 4 On the Step 2 Restore—Choose the Backup Tar File page, in Select Backup File field, select the backup file that you want to restore and select **Next**.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 In the Step 3 Restore—Select the Type of Restore page, under Special Features, check the check boxes for the features that you want to restore and select **Next**.

Note Only the features that were backed up to the file that you chose will appear on the page.

Step 6 In the Step 4 Restore—Final Warning for Restore page, in the Select the Server field, select the publisher server and select **Restore**.

Caution The publisher server must have the same IP address and hostname as the server from which Disaster Recovery System backed up the data. Otherwise, Disaster Recovery System Disaster Recovery System will not restore the data.

Note During the restore process, do not perform any tasks with Connection Administration.

Step 7 When the restore status indicates 100 percent, restart the publisher server.

To Install the Replacement Subscriber Server or Hard Disks

Step 1 Shut down the subscriber server.

Step 2 If you are replacing the subscriber server, disconnect the network cable from the old subscriber server and connect it to the new subscriber server.

If you are replacing the hard disks, do the procedure in the "Installing Replacement Hard Disks in a Connection 7.x Server" section on page 7-17.

Step 3 Reinstall Connection. Follow the instructions in "Part 3: Configuring the Cluster, and Installing and Configuring the Subscriber Connection Server" in the "Task List for Installing a Cisco Unity Connection 7.x system with a Connection Cluster Configured" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

When you reinstall Connection, note the following:

- You must install the same software and ES version that is installed on the publisher server. Otherwise, the Connection cluster may not function correctly.
- You must specify the same security password as the security password for the publisher server. Otherwise, the Connection cluster will not function. If you do not know the security password, you can change it on the publisher server before you install the subscriber server by using the CLI command **set password user**. For more information, see the applicable version of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
- Only when you are replacing the server (not when you are replacing only the hard disks), you must install a replacement license that includes the MAC address of the replacement subscriber server. Otherwise, Connection will not function.

To Copy the Data from the Publisher Server to the Subscriber Server

Step 1 Sign in to the command-line interface (CLI) for the subscriber server.

Step 2 Run the CLI command **utils cuc cluster overwritedb** to force Connection to copy data from the publisher server to the subscriber server:

Step 3 Run the CLI command **show cuc cluster status** to confirm that the new Connection cluster has been configured correctly on the subscriber server.

Step 4 Sign in to the CLI for the publisher server.

Step 5 Run the CLI command **show cuc cluster status** to confirm that the new Connection cluster has been configured correctly on the publisher server.

To Synchronize MWIs for Each Phone System

Step 1 During off-peak hours, sign in to either server in the Connection cluster.

Step 2 In Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

Step 3 On the Search Phone Systems page, select the name of the first phone system.

Step 4 On the Phone System Basics page, under Messaging Waiting Indicators, select **Run**.

Step 5 Select **Next**.

Step 6 Repeat Step 4 and Step 5 for the remaining phone systems.

Installing Replacement Hard Disks in a Connection 7.x Server

Added March 4, 2010

Use the procedure in this section to replace all hard disks in the server with blank disks as part of an installation or upgrade.

Caution Do not replace hard disks in the Connection server with disks that contain data, even if the replacement disks were originally disks in the same RAID in the same server.

Caution The procedure in this section is just one part of the process of replacing hard disks in a Connection server. When replacing hard disks in a Connection server, refer to the applicable task list earlier in this chapter, or Connection may not function correctly.

Warning **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.** Statement 1

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.** Statement 2

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.** Statement 88

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.** Statement 117

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**
• This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
• When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
• If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.** Statement 1021

Warning **To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

(For translations of the preceding safety warnings, see *Regulatory Compliance and Safety Information for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/regulatory/compliance/ucwarns.html.)

To Install Replacement Hard Disks in a Connection 7.x Server

Step 1 Remove the cover.

Step 2 Replace all of the hard disks in the server:

Caution If you are replacing hard disks as part of a Connection installation or upgrade, you must remove all existing hard disks and install exactly as many hard disks as you remove, or the Connection installation or upgrade will fail.

a. Make note of the current locations of the hard disks in the server, including which hard disk is in which hard disk slot. If the replacement fails and you want to revert to the current configuration, you must put the existing hard disks back into their current locations.

b. Remove the drive trays from the server.

c. Remove the old hard disks from the drive trays.

d. Insert the new hard disks into the drive trays.

e. Reinstall the drive trays in the locations that you made note of in Step a.

Step 3 Reattach the cover.

CHAPTER 8

Creating or Changing a Cisco Unity Connection 7.x Cluster

This chapter contains the following sections:

Adding a 7.x Server to Create a Connection Cluster

When you have a single Connection server, you can add a subscriber server and create a Connection cluster.

Do the three procedures in this section in the order listed.

To Install the Subscriber Server

Follow the instructions in "Part 3: Configuring the Cluster, and Installing and Configuring the Subscriber Connection Server" in the "Task List for Installing a Cisco Unity Connection 7.x system with a Connection Cluster Configured" in the "Overview of Mandatory Tasks for Installing a Cisco Unity Connection 7.x System" chapter of the *Installation Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/installation/guide/7xcucigx.html.

Caution Both Connection servers must have the same software and ES versions installed. Otherwise, the Connection cluster may not function correctly.

To Configure the Phone System for the Connection Cluster

See the applicable documentation, depending on the phone system integration type:

Integration by Skinny Client Control Protocol (SCCP) with Cisco Unified Communications Manager

a. To add the ports on the phone system that will connect to the subscriber server, see the "Adding Ports to an Existing Cisco Voice-Mail Server" section in the "Cisco Voice Mail Port Wizard" chapter of the applicable *Cisco Unified Communications Manager Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

b. To set the Distribution Algorithm field to Top Down for the line group of the answering voicemail ports, see the "Configuring a Line Group" section in the "Line Group Configuration" chapter of the applicable *Cisco Unified Communications Manager Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Integration by Skinny Client Control Protocol (SCCP) with Cisco Unified Communications Manager Express

To add the ports on the phone system that will connect to the subscriber server, see the "How to Configure Voice-Mail Integration" section in the "Integrating Voice Mail" chapter of the *Cisco Unified Communications Manager Express System Administrator Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html.

Integration through a SIP trunk with Cisco Unified Communications Manager

See the "Programming the Cisco Unified Communications Manager Phone System for Integrating with Cisco Unity Connection" section of the *Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection 7.x* at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guide.

Integration through a SIP trunk with Cisco Unified Communications Manager Express

See the "Programming the Cisco Unified Communications Manager Express Phone System for Integrating with Cisco Unity Connection" section of the *Cisco Unified Communications Manager Express SIP Trunk Integration Guide for Cisco Unity Connection 7.x* at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Integration through PIMG/TIMG units

See the "Setting Up the PIMG Units" or "Setting Up the TIMG Units" section of the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Other integrations that use SIP

See the "Programming the <Phone System>" section of the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

To Configure Cisco Unity Connection for the Cluster

See the applicable documentation, depending on the phone system integration:

Cisco Unified CM and Cisco Unified CM Express integrations

To add voice messaging ports to the applicable port group on the publisher server, see the "Managing Ports" section in the "Managing the Phone System Integrations" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Note The total number of ports on the Connection server must not exceed the number of ports enabled by the Cisco Unity Connection license.

All phone system integrations except for PIMG/TIMG integrations

To configure the ports on the publisher server, see the "Creating the Integration with the <Phone System>" section of the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Converting a 7.x Publisher Server to a Single Server Without a Connection Cluster

You can remove the subscriber server from a Connection cluster so that you undo the Connection cluster. The publisher server becomes a single server without a Connection cluster, and the subscriber server is removed from the network. (To use the subscriber server as a single server without a Connection cluster, you must reinstall Connection on the server.)

Note You cannot remove the publisher server from a Connection cluster.

Do the five procedures in this section in the order listed.

To Manually Change the Publisher Server to Primary Status

Step 1 Log on to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, click **Cluster Management**.

Step 3 On the Cluster Management page, under Server Manager, locate the publisher server.

Step 4 If the publisher server has Primary status, skip the remaining steps in this procedure and skip to the next procedure.

If the publisher server has Secondary status, skip to Step 5.

If the publisher has Deactivated status, change the status to Secondary:

a. In the Change Server Status column for the publisher server, click **Activate**.

b. When prompted to confirm changing the server status, click **OK**.

c. Confirm that the Server Status column indicates that the publisher server now has Secondary status.

Step 5 In the Change Server Status column for the publisher server, click **Make Primary**.

Step 6 When prompted to confirm changing the server status, click **OK**.

The Server Status column displays the changed status when the change is complete.

Note The subscriber server will automatically change to Secondary status.

To Manually Change the Subscriber Server from Secondary Status to Deactivated Status

Step 1 Log on to the Real-Time Monitoring Tool (RTMT).

Step 2 On the Cisco Unity Connection menu, click **Port Monitor**. The Port Monitor tool appears in the right pane.

Step 3 In the Node field, click the subscriber server.

Step 4 In the right pane, click **Start Polling**.

Step 5 Note whether any voice messaging ports are currently handling calls for the server.

Step 6 If no voice messaging ports are currently handling calls for the server, skip to Step 7.

If there are voice messaging ports that are currently handling calls for the server, in Cisco Unity Connection Serviceability, on the Cluster Management page, under Change Port Status, click **Stop Taking Calls** for the subscriber server, then wait until RTMT shows that all ports for the subscriber server are idle.

Step 7 In Cisco Unity Connection Serviceability, on the Cluster Management page, under Server Manager, in the Change Server Status column for the subscriber server, click **Deactivate**.

Step 8 When prompted to confirm changing server status, click **OK**.

The Server Status column displays the changed status for the subscriber server when the change is complete.

To Remove the Subscriber Server from the Environment

Step 1 Shut down the subscriber server.

The Server Status column shows the subscriber server has Not Functioning status.

Step 2 Disconnect the network cable from the subscriber server.

The subscriber server can be removed from the environment.

To Remove the Subscriber Server from the Cluster

Step 1 On the publisher server, log on to Cisco Unity Connection Administration.

Step 2 In Cisco Unity Connection Administration, expand **System Settings**, then click **Cluster**.

Step 3 On the Find and List Servers page, click **Find** to display all servers in the cluster.

Step 4 Check the check box in front of the name for the subscriber server and click **Delete Selected**.

Step 5 When prompted to confirm deleting the server, click **OK**.

To Ensure That All Calls Go to the Remaining Connection Server

See the applicable documentation, depending on the phone system integration type:

Integration by Skinny Client Control Protocol (SCCP) with Cisco Unified Communications Manager

a. To delete the ports on the phone system that connected to the subscriber server, see the *Cisco Unified Communications Manager Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

b. Configure the hunt group for the voice mail ports on the phone system to send calls only to the remaining server (the publisher).

Integration by Skinny Client Control Protocol (SCCP) with Cisco Unified Communications Manager Express

a. To delete the ports on the phone system that connected to the subscriber server, see the *Cisco Unified Communications Manager Express System Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html.

b. Configure the hunt group for the voice mail ports on the phone system to send calls only to the remaining server (the publisher).

Integration through a SIP trunk with Cisco Unified Communications Manager

To configure the hunt group for the voice mail ports on the phone system to send calls only to the remaining server (the publisher), see the *Cisco Unified Communications Manager Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Integration through a SIP trunk with Cisco Unified Communications Manager Express

To configure the hunt group for the voice mail ports on the phone system to send calls only to the remaining server (the publisher), see the *Cisco Unified Communications Manager Express System Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html.

Integration through PIMG/TIMG units

To configure the PIMG/TIMG units to send all calls to the remaining server (the publisher), see the "Setting Up the PIMG Units" or "Setting Up the TIMG Units" section of the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Other Integrations That Use SIP

To configure the hunt group for the voice mail ports on the phone system to send calls only to the remaining server (the publisher), see the phone system documentation.

CHAPTER 9

Changing the IP Addresses of Cisco Unity Connection 7.x Servers

This chapter contains the following sections:

Determining Whether a Connection 7.x Server Is Defined by a Host Name or an IP Address

Revised June 5, 2009

The procedure you use to change the IP address of a Connection server depends on whether the server is defined by a host name or by an IP address.

To Determine Whether a Connection 7.x Server Is Defined by a Host Name or an IP Address

Step 1 On the server whose IP address you want to change, log onto Cisco Unity Connection Administration.

Step 2 Expand System Settings, and click **Cluster**.

You go to the Cluster page even when no cluster is configured.

Step 3 Click **Find** to display a list of servers in the cluster.

Step 4 For the server whose IP address you want to change, if the value of the Host Name/IP Address column is a host name, the server is defined by a host name.

If the value of the Host Name/IP Address column is an IP address, the server is defined by an IP address.

Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed

When you change the IP address of the Connection server, you must also make the same change on all associated components that reference the Connection server by IP address:

- Bookmarks on client computers to the following web applications:
  - Cisco Personal Communications Assistant
  - Cisco Unity Connection Administration
  - Real-Time Monitoring Tool
- Cisco Fax Server
- Cisco Unified Application Environment
- Cisco Unified Mobile Advantage
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- Cisco Unity Connection ViewMail for Microsoft Outlook
- IMAP e-mail clients that access Connection
- Phone systems and related components:
  - Cisco EGW 2200
  - Cisco ISR voice gateway
  - Cisco SIP Proxy Server
  - Cisco Unified Communications Manager
  - Cisco Unified Communications Manager Express
  - PIMG/TIMG units
- RSS readers
- SMTP smart host
- Voice-messaging systems with which Connection is integrated via VPIM, including:
  - Cisco Unity
  - Cisco Unity Express

Changing the IP Address of a Single 7.x Server That Is Defined by a Hostname (No Connection Cluster)

Revised June 5, 2009

Caution Do not change the IP address of a Connection server during business hours. The server must be restarted for changes to take effect.

To Change the IP Address of a Single 7.x Server That Is Defined by a Hostname (No Connection Cluster)

Step 1 Review the list of associated components on which you also need to change the IP address of the Connection server if those components reference Connection by IP address. See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Caution If associated components reference the Connection server by IP address and if you do not change the IP address as applicable, the components will no longer be able to access the Connection server.

Step 2 In the Real-Time Monitoring Tool (RTMT) confirm that the server is running and available:

a. Using the RTMT, log onto the server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step 3.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

Step 3 Log on to Cisco Unified Serviceability, and check the status of the server:

a. From the Tools menu, click **Cluster Management**.

b. In the Server Status column, confirm that the value for the current server is Primary. If the Server Status column has any other value, resolve the problem before continuing.

Step 4 Check network connectivity and DNS server configuration by running the following CLI command:

```
admin: utils diagnose module validate_network

Log file: /var/log/active/platform/log/diag1.log


Starting diagnostic test(s)

===========================

test - validate_network    : Passed


Diagnostics Completed

admin:
```

Step 5 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Step 6 If Digital Networking is configured, remove the server from the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Caution Readding a server to a digital network can be a time-consuming process. Ensure that you thoroughly understand the work required to readd a server to a digital network before you continue with this procedure.

Step 7 On a DNS server, change the DNS record of the server to the new IP address. Update both the forward (A) and reverse (PTR) records.

Step 8 Change the IP address of the server and, if applicable, the default gateway:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **IP > Ethernet**.

c. Under Port Information, change the value of the IP Address field and, if applicable, the Subnet Mask field.

d. If you are moving the server to a different subnet that requires a new default gateway address, under Gateway Information, change the value of the Default Gateway field.

e. Click **Save**, and the system restarts.

Step 9 In the RTMT, confirm that the server is running and available:

a. Using the RTMT, log on to the server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step 10.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

Step 10 Update RTMT custom alerts and saved profiles.

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure the custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and readd the counters and then save the profiles to update them to the new IP address.

Step 11 Check associated components and change configurations as required. (Consult documentation for the affected products to determine how to make the required changes.) See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Step 12 If the server was part of a digital network before you changed the IP address, readd the server to the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Step 13 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Changing the IP Address of a Single 7.x Server That Is Defined by an IP Address (No Connection Cluster)

Added June 5, 2009

Caution Do not change the IP address of a Connection server during business hours. The server must be restarted for changes to take effect.

To Change the IP Address of a Single 7.x Server That Is Defined by an IP Address (No Connection Cluster)

Step 1 Review the list of associated components on which you also need to change the IP address of the Connection server if those components reference Connection by IP address. See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Caution If associated components reference the Connection server by IP address and if you do not change the IP address as applicable, the components will no longer be able to access the Connection server.

Step 2 In the Real-Time Monitoring Tool (RTMT) confirm that the server is running and available:

a. Using the RTMT, log onto the server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step 3.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

Step 3 Log on to Cisco Unified Serviceability, and check the status of the server:

a. From the Tools menu, click **Cluster Management**.

b. In the Server Status column, confirm that the value for the current server is Primary. If the Server Status column has any other value, resolve the problem before continuing.

Step 4 Check network connectivity and DNS server configuration by running the following CLI command:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)
===========================
test - validate_network    : Passed

Diagnostics Completed
admin:
```

Step 5 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Step 6 If Digital Networking is configured, remove the server from the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Caution Readding a server to a digital network can be a time-consuming process. Ensure that you thoroughly understand the work required to readd a server to a digital network before you continue with this procedure.

Step 7 On a DNS server, change the DNS record of the server to the new IP address. Update both the forward (A) and reverse (PTR) records.

Step 8 Change the IP addresses of the server in Connection Administration:

a. Log on to Cisco Unity Connection Administration.

b. Expand System Settings, and click **Cluster**.

c. Click **Find** to display a list of servers in the cluster.

d. Click the name of the server.

e. Change the value of the Host Name/IP Address field to the new IP address.

f. Click **Save**.

Step 9 Change the IP address of the server and, if applicable, the default gateway:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **IP > Ethernet**.

c. Under Port Information, change the value of the IP Address field and, if applicable, the Subnet Mask field.

d. If you are moving the server to a different subnet that requires a new default gateway address, under Gateway Information, change the value of the Default Gateway field.

e. Click **Save**, and the system restarts.

Step 10 In the RTMT, confirm that the server is running and available:

a. Using the RTMT, log on to the server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step 10.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

Step 11 Update RTMT custom alerts and saved profiles.

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure the custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and readd the counters and then save the profiles to update them to the new IP address.

Step 12 Check associated components and change configurations as required. (Consult documentation for the affected products to determine how to make the required changes.) See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Step 13 If the server was part of a digital network before you changed the IP address, readd the server to the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Step 14 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Changing the IP Address of a 7.x Publisher Server That Is Defined by a Host Name

Caution Do not change the IP address of a Connection server during business hours. When a Connection cluster is configured, both servers must be restarted for changes to take effect.

To Change the IP Address of a 7.x Publisher Server that Is Defined by a Host Name

Step 1 Review the list of associated components on which you also need to change the IP address of the Connection server if those components reference Connection by IP address. See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Caution If associated components reference the Connection server by IP address and if you do not change the IP address as applicable, the components will no longer be able to access the Connection server.

Step 2 In the Real-Time Monitoring Tool (RTMT), confirm that the publisher and subscriber servers are running and available:

a. Using the RTMT, log on to the publisher server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step d.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

d. Repeat Step a. through Step c. on the subscriber server.

Step 3 On the publisher server, log on to Cisco Unified Serviceability, and check the status of the server:

a. From the Tools menu, click **Cluster Management**.

b. In the Server Status column, confirm that the value for the current server is either Primary or Secondary. If the Server Status column has any other value, resolve the problem before continuing.

Step 4 Check network connectivity and DNS server configuration by running the following CLI command:

admin: utils diagnose module validate_network

Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)

==========

test - validate_network : Passed

Diagnostics Completed

admin:

Step 5 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Step 6 If Digital Networking is configured, remove the publisher server from the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Caution Readding a server to a digital network can be a time-consuming process. Ensure that you thoroughly understand the work required to readd a server to a digital network before you continue with this procedure.

Step 7 On a DNS server, change the DNS record of the publisher server to the new IP address. Update both the forward (A) and reverse (PTR) records.

Step 8 On the subscriber server, change the IP address of the publisher server:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **IP > Publisher**.

c. Change the IP address of the publisher server.

d. Click **Save**.

Step 9 On the publisher server, change the IP address of the publisher server and, if applicable, the default gateway:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **IP > Ethernet**.

c. Under Port Information, change the value of the IP Address field and, if applicable, the Subnet Mask field.

d. If you are moving the publisher server to a different subnet that requires a new default gateway address, under Gateway Information, change the value of the Default Gateway field.

e. Click **Save**, and the system restarts.

Step 10 Log on to the subscriber server by using an SSH application, and run the CLI command **utils system restart** to restart the server, which updates the local name resolution files.

Step 11 In the RTMT, confirm that the publisher and subscriber servers are running and available:

a. Using the RTMT, log on to the publisher server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step d.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

d. Repeat Step a. through Step c. on the subscriber server.

Step 12 Update RTMT custom alerts and saved profiles.

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure the custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and readd the counters and then save the profiled to update them to the new IP address.

Step 13 Check associated components and change configurations as required. (Consult documentation for the affected products to determine how to make the required changes.) See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Step 14 If the publisher server was part of a digital network before you changed the IP address of this server, readd the server to the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Step 15 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Changing the IP Address of a 7.x Publisher Server That Is Defined by an IP Address

Caution Do not change the IP address of a Connection server during business hours. When a Connection cluster is configured, both servers must be restarted for changes to take effect.

To Change the IP Address of a 7.x Publisher Server that Is Defined by an IP Address

Step 1 Review the list of associated components on which you also need to change the IP address of the Connection server if those components reference Connection by IP address. See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Caution If associated components reference the Connection server by IP address and if you do not change the IP address as applicable, the components will no longer be able to access the Connection server.

Step 2 In the Real-Time Monitoring Tool (RTMT), confirm that the publisher and subscriber servers are running and available:

a. Using the RTMT, log on to the publisher server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step d.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

d. Repeat Step a. through Step c. on the subscriber server.

Step 3 On the publisher server, log on to Cisco Unified Serviceability, and check the status of the server:

a. From the Tools menu, click **Cluster Management**.

b. In the Server Status column, confirm that the value for the current server is either Primary or Secondary. If the Server Status column has any other value, resolve the problem before continuing.

Step 4 Check network connectivity and DNS server configuration by running the following CLI command:

```
admin: utils diagnose module validate_network

Log file: /var/log/active/platform/log/diag1.log


Starting diagnostic test(s)

============================

test - validate_network    : Passed


Diagnostics Completed

admin:
```

Step 5 If Digital Networking is configured, remove the publisher server from the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Caution Readding a server to a digital network can be a time-consuming process. Ensure that you thoroughly understand the work required to readd a server to a digital network before you continue with this procedure.

Step 6 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Step 7 On the publisher server, change the IP addresses of the publisher server in Connection Administration:

a. Log on to Cisco Unity Connection Administration.

b. Expand System Settings, and click **Cluster**.

c. Click **Find** to display a list of servers in the cluster.

d. Click the name of the publisher server.

e. Change the value of the Host Name/IP Address field to the new IP address.

f. Click **Save**.

Step 8 On the publisher server, change the IP address of the publisher server and, if applicable, the default gateway in Cisco Unified Operating System Administration:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **IP > Ethernet**.

c. Under Port Information, change the value of the IP Address field and, if applicable, the Subnet Mask field.

d. If you are moving the publisher server to a different subnet that requires a new default gateway address, under Gateway Information, change the value of the Default Gateway field.

e. Click **Save**, and the system restarts.

Step 9 On the subscriber server, change the IP address of the publisher server:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **IP > Publisher**.

c. Change the IP address of the publisher server.

d. Click **Save**.

Step 10 Log on to the subscriber server by using an SSH application, and run the CLI command **utils system restart** to restart the server, which updates the local name resolution files.

Step 11 In the RTMT, confirm that the publisher and subscriber servers are running and available:

a. Using the RTMT, log on to the publisher server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step d.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

d. Repeat Step a. through Step c. on the subscriber server.

Step 12 Update RTMT custom alerts and saved profiles.

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure the custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and readd the counters and then save the profiles to update them to the new IP address.

Step 13 Check associated components and change configurations as required. (Consult documentation for the affected products to determine how to make the required changes.) See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Step 14 If the publisher server was part of a digital network before you changed the IP address of this server, readd the server to the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Step 15 Back up the server using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Changing the IP Address of a 7.x Subscriber Server That Is Defined by a Host Name

Caution Do not change the IP address of a Connection server during business hours. When a Connection cluster is configured, both servers must be restarted for changes to take effect.

To Change the IP Address of a 7.x Subscriber Server that Is Defined by a Host Name

Step 1 Review the list of associated components on which you also need to change the IP address of the Connection server if those components reference Connection by IP address. See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Caution If associated components reference the Connection server by IP address and if you do not change the IP address as applicable, the components will no longer be able to access the Connection server.

Step 2 In the Real-Time Monitoring Tool (RTMT), confirm that the publisher and subscriber servers are running and available:

a. Using the RTMT, log on to the publisher server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step d.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

d. Repeat Step a. through Step c. on the subscriber server.

Step 3 On the subscriber server, log on to Cisco Unified Serviceability, and check the status of the server:

a. From the Tools menu, click **Cluster Management**.

b. In the Server Status column, confirm that the value for the current server is either Primary or Secondary. If the Server Status column has any other value, resolve the problem before continuing.

Step 4 Check network connectivity and DNS server configuration by running the following CLI command:

admin: utils diagnose module validate_network

Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)

==========

test - validate_network : Passed

Diagnostics Completed

admin:

Step 5 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Step 6 On a DNS server, change the DNS record of the subscriber server to the new IP address. Update both the forward (A) and reverse (PTR) records.

Step 7 Confirm that the DNS change propagates to the publisher server by using the following two CLI commands on the subscriber server and the publisher server:

utils network host

show tech network hosts

Step 8 On the subscriber server, change the IP address of the subscriber server and, if applicable, the default gateway:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **IP > Ethernet**.

c. Under Port Information, change the value of the IP Address field and, if applicable, the Subnet Mask field.

d. If you are moving the publisher server to a different subnet that requires a new default gateway address, under Gateway Information, change the value of the Default Gateway field.

e. Click **Save**, and the system restarts.

Step 9 Log on to the publisher server by using an SSH application, and run the CLI command **utils system restart** to restart the server, which updates the local name resolution files.

Step 10 In the RTMT, confirm that the publisher and subscriber servers are running and available:

a. Using the RTMT, log on to the publisher server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step d.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

d. Repeat Step a. through Step c. on the subscriber server.

Step 11 Update RTMT custom alerts and saved profiles.

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure the custom alerts.

- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and readd the counters and then save the profiles to update them to the new IP address.

Step 12 Check associated components and change configurations as required. (Consult documentation for the affected products to determine how to make the required changes.) See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Step 13 Back up the publisher server using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Changing the IP Address of a 7.x Subscriber Server That Is Defined by an IP Address

Caution Do not change the IP address of a Connection server during business hours. When a Connection cluster is configured, both servers must be restarted for changes to take effect.

To Change the IP Address of a 7.x Subscriber Server that Is Defined by an IP Address

Step 1 Review the list of associated components on which you also need to change the IP address of the Connection server if those components reference Connection by IP address. See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Caution If associated components reference the Connection server by IP address and if you do not change the IP address as applicable, the components will no longer be able to access the Connection server.

Step 2 In the Real-Time Monitoring Tool (RTMT), confirm that the publisher and subscriber servers are running and available:

a. Using the RTMT, log on to the publisher server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step d.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

d. Repeat Step a. through Step c. on the subscriber server.

Step 3 On the subscriber server, log on to Cisco Unified Serviceability, and check the status of the server:

a. From the Tools menu, click **Cluster Management**.

b. In the Server Status column, confirm that the value for the current server is either Primary or Secondary. If the Server Status column has any other value, resolve the problem before continuing.

Step 4 Check network connectivity and DNS server configuration by running the following CLI command:

admin: utils diagnose module validate_network

Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)

==========

test - validate_network : Passed

Diagnostics Completed

admin:

Step 5 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

Step 6 On the publisher server, change the IP addresses of the subscriber server:

a. Log on to Cisco Unity Connection Administration.

b. Expand System Settings, and click **Cluster**.

c. Click **Find** to display a list of servers in the cluster.

d. Click the name of the subscriber server.

e. Change the value of the Host Name/IP Address field to the new IP address.

f. Click **Save**.

Step 7 On the subscriber server, change the IP address of the subscriber server and, if applicable, the default gateway:

a. Log on to Cisco Unified Operating System Administration.

b. From the Settings menu, click **IP > Ethernet**.

c. Under Port Information, change the value of the IP Address field and, if applicable, the Subnet Mask field.

d. If you are moving the publisher server to a different subnet that requires a new default gateway address, under Gateway Information, change the value of the Default Gateway field.

e. Click **Save**, and the system restarts.

Step 8 Log on to the publisher server by using an SSH application, and run the CLI command **utils system restart** to restart the server, which updates the local name resolution files.

Step 9 In the RTMT, confirm that the publisher and subscriber servers are running and available:

a. Using the RTMT, log on to the publisher server.

b. In the left pane, under Tools, click **Alert Central**.

c. In the right pane, on the System tab, if ServerDown is black, skip to Step d.

If ServerDown is red, right-click **ServerDown**, and click **Alert Details**. Resolve the problem before continuing.

d. Repeat Step a. through Step c. on the subscriber server.

Step 10 Update RTMT custom alerts and saved profiles.

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure the custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and readd the counters and then save the profiles to update them to the new IP address.

Step 11 Check associated components and change configurations as required. (Consult documentation for the affected products to determine how to make the required changes.) See the "Associated Components on Which the IP Address of a Connection 7.x Server Must Be Changed" section on page 9-2.

Step 12 Back up the server by using the Disaster Recovery System. See the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/drs_administration/guide/7xcucdrsag.html.

CHAPTER 10

Renaming Cisco Unity Connection 7.x Servers

This chapter contains the following sections:

Renaming a Single 7.x Server Without a Connection Cluster

Revised May 2009

Do the following tasks to change the host name of a single Connection server without a cluster.

1. *If you created and installed an SSL certificate on the server that you are renaming*: Create a new certificate signing request, and get a new signed certificate before you begin to rename the server.

Note If you do not get a new signed certificate before you rename the server, when you use web applications to access the Connection server, a security alert displays and explains that there is a problem with the security certificate.

   a. Run the CLI command **set web-security** to assign an alternate host name to the server that you are renaming. See the `set web-security` command in the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

   b. Create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external certification authority (CA). Do the "To Create and Download a Certificate Signing Request" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

   c. If you are using Microsoft Certificate Services to export the root certificate and issue the server certificate, do the "To Export the Root Certificate and Issue the Server Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and

IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

If you are using another application to issue the certificate, see the documentation for the application for information on issuing certificates.

If you are using an external CA to issue the certificate, send the certificate signing request to the external CA. When the external CA returns the certificate, continue with Step 2.

2. If Digital Networking is configured, remove the server from the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Caution Re-adding a server to a digital network can be a time-consuming process. Ensure that you thoroughly understand the work required to re-add a server to a digital network before you begin this procedure.

3. Rename the server. Do the "To Rename a Single 7.x Server Without a Connection Cluster" procedure on page 10-2.
4. *If you created and installed an SSL certificate on the server that you are renaming*: Upload the root certificate and the server certificate to the Connection server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Connection Server" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
5. *If you created and installed an SSL certificate on the server that you are renaming*: Restart the Connection IMAP Server service so that Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Connection IMAP Server Service" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
6. *If the server was part of a digital network before you renamed the server*: Re-add the server to the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Rename a Single 7.x Server Without a Connection Cluster

Step 1 On a DNS server, change the DNS record of the Connection server to the new host name.

Step 2 Confirm that the DNS change propagates to the server. Log on to the server by using an SSH application, and run the CLI command **utils network host <hostname>**.

Do not proceed if the new host name does not resolve to the correct IP address.

Step 3 *Optional:* On the Connection server, change the SMTP domain in Cisco Unity Connection Administration:

a. Expand **System Settings > SMTP Configuration**, and click **Server**.

b. Click **Change SMTP Domain**, and change the value of the SMTP Domain field.

c. Click **Save**.

Step 4 In Connection Administration, change the host name of the server:

a. Expand **System Settings**, and click **Cluster**.

b. Click **Find** to display a list of servers.

c. Click the host name of the server that you want to rename.

d. On the Server Configuration page, change the value of the **Host Name/IP Address** field to the new name.

e. Click **Save**.

Step 5 In Cisco Unified Operating System Administration, change the host name of the server:

a. From the Settings menu, click **IP > Ethernet**.

b. Change the host name of the Connection server.

c. Click **Save**. The server automatically restarts.

Step 6 Log on to the server by using an SSH application, and run the CLI command **utils system restart** to restart the server.

Renaming the 7.x Publisher Server in a Connection Cluster

Revised May 2009

Do the following tasks to change the host name of the publisher server in a Connection cluster.

1. *If you created and installed an SSL certificate on the server that you are renaming*: Create a new certificate signing request, and get a new signed certificate before you begin to rename the server.

Note If you do not get a new signed certificate before you rename the server, when you use web applications to access the Connection server, a security alert displays and explains that there is a problem with the security certificate.

a. Run the CLI command **set web-security** to assign an alternate host name to the server that you are renaming. See the `set web-security` command in the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

b. Create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external certification authority (CA). Do the "To Create and Download a Certificate Signing Request" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release*

7.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

c. If you are using Microsoft Certificate Services to export the root certificate and issue the server certificate, do the "To Export the Root Certificate and Issue the Server Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

If you are using another application to issue the certificate, see the documentation for the application for information on issuing certificates.

If you are using an external CA to issue the certificate, send the certificate signing request to the external CA. When the external CA returns the certificate, continue with Step 2.

2. If Digital Networking is configured, remove the server from the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Caution Re-adding a server to a digital network can be a time-consuming process. Ensure that you thoroughly understand the work required to re-add a server to a digital network before you begin this procedure.

3. Rename the server. Do the "To Rename the 7.x Publisher Server in a Connection Cluster" procedure on page 10-5.
4. *If you created and installed an SSL certificate on the server that you are renaming*: Upload the root certificate and the server certificate to the Connection server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Connection Server" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
5. *If you created and installed an SSL certificate on the server that you are renaming*: Restart the Connection IMAP Server service so that Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Connection IMAP Server Service" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
6. *If the server was part of a digital network before you renamed the server*: Re-add the server to the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Rename the 7.x Publisher Server in a Connection Cluster

Step 1 On a DNS server, change the DNS record of the publisher server to the new host name.

Step 2 Confirm that the DNS change propagates to the publisher server. Log on to the publisher server by using an SSH application, and run the CLI command **utils network host <hostname>**.

Do not proceed if the new host name does not resolve to the correct IP address.

Step 3 Repeat Step 2 on the subscriber server.

Step 4 *Optional:* On the publisher server, change the SMTP domain in Cisco Unity Connection Administration:

a. Expand **System Settings > SMTP Configuration**, and click **Server**.

b. Click **Change SMTP Domain**, and change the value of the SMTP Domain field.

c. Click **Save**.

Step 5 On the publisher server, change the host name of the publisher server in Connection Administration:

a. Expand **System Settings**, and click **Cluster**.

b. Click **Find** to display a list of servers.

c. Click the host name of the server that you want to rename.

d. On the Server Configuration page, change the value of the **Host Name/IP Address** field to the new name.

e. Click **Save**.

Step 6 On the subscriber server, change the name by which the subscriber server knows the publisher server:

a. In Cisco Unified Operating System Administration, from the Settings menu, click **IP > Publisher**.

b. Change the host name of the publisher server.

c. Click **Save**.

Log on to the subscriber server by using an SSH application, and run the CLI command **utils system restart** to restart the server.

Step 7 On the publisher server, change the name of the publisher server in Cisco Unified Operating System Administration.

a. From the Settings menu, click **IP > Ethernet**.

b. Change the host name of the publisher server.

c. Click **Save**. The publisher server automatically restarts.

d. Wait for the publisher server to finish restarting. When you can log on to Connection Administration on the publisher server, continue with Step 8.

Step 8 Log on to the subscriber server by using an SSH application, and run the CLI command **utils system restart** to restart the server.

Step 9 Wait for the subscriber server to finish restarting. When you can log on to Connection Administration on the subscriber server, continue with Step 10.

Step 10 On the publisher server, run the CLI command **utils dbreplication reset all** to reset replication.

Step 11 Wait until the replication reset process is complete. To determine when the process is completed:

a. Log on to Real-Time Monitoring Tool (RTMT) by connecting to the publisher server.

b. On the System menu, click **Performance > Open Performance Monitoring**.

c. In the right pane, expand **Number of Replicates Created and State of Replication**, then double-click **Replicate_State**.

d. In the Object Instances dialog box, click **ReplicateCount** and click **Add**.

e. Wait until the value reaches **2.0**.

   For more information on possible values and their meaning, right-click **Replicate_State**, and click **Counter Description**.

f. On the File menu, click **Exit** to exit RTMT.

Step 12 Log on to the publisher server by using an SSH application, and run the CLI command **utils system restart** to restart the server.

This command causes the Connection cluster servers to change server status so the publisher server has the Secondary status and the subscriber server has the Primary status.

Step 13 Run the CLI command **utils cuc cluster makeprimary <name_of_publisher_server>** to change the publisher server to Primary status.

Renaming the 7.x Subscriber Server in a Connection Cluster

Revised May 2009

Use the following task list to change the host name of the subscriber server in a Connection cluster.

1. *If you created and installed an SSL certificate on the server that you are renaming*: Create a new certificate signing request, and get a new signed certificate before you begin to rename the server.

Note If you do not get a new signed certificate before you rename the server, when you use web applications to access the Connection server, a security alert displays and explains that there is a problem with the security certificate.

   a. Run the CLI command **set web-security** to assign an alternate host name to the server that you are renaming. See the `set web-security` command in the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

   b. Create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external certification authority (CA). Do the "To Create and Download a Certificate Signing Request" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

   c. If you are using Microsoft Certificate Services to export the root certificate and issue the server certificate, do the "To Export the Root Certificate and Issue the Server Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration*

Guide for Cisco Unity Connection Release 7.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

If you are using another application to issue the certificate, see the documentation for the application for information on issuing certificates.

If you are using an external CA to issue the certificate, send the certificate signing request to the external CA. When the external CA returns the certificate, continue with Step 2.

2. If Digital Networking is configured, remove the server from the digital network. See the "Using Digital Networking" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

Caution Re-adding a server to a digital network can be a time-consuming process. Ensure that you thoroughly understand the work required to re-add a server to a digital network before you begin this procedure.

3. Rename the server. Do the "To Rename the 7.x Subscriber Server in a Connection Cluster" procedure on page 10-7.
4. *If you created and installed an SSL certificate on the server that you are renaming*: Upload the root certificate and the server certificate to the Connection server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Connection Server" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.
5. *If you created and installed an SSL certificate on the server that you are renaming*: Restart the Connection IMAP Server service so that Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Connection IMAP Server Service" procedure in the "Creating and Installing an SSL Server Certificate" section in the "Securing Cisco PCA and IMAP Email Client Access to Cisco Unity Connection" chapter of the *System Administration Guide for Cisco Unity Connection Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/administration/guide/7xcucsagx.html.

To Rename the 7.x Subscriber Server in a Connection Cluster

Step 1 On a DNS server, change the DNS record of the subscriber server to the new host name.

Step 2 Confirm that the DNS change propagates to the publisher server. Log on to the publisher server by using an SSH application, and run the CLI command **utils network host <hostname>**.

Do not proceed if the new host name does not resolve to the correct IP address.

Step 3 Repeat Step 2 on the subscriber server.

Step 4 On the publisher server, change the name by which the publisher server knows the subscriber server:

a. In Cisco Unity Connection Administration, expand **System Settings**, and click **Cluster**.
b. Click **Find** to display a list of servers.

c. Click the host name of the subscriber server.

d. On the Server Configuration page, change the value of the **Host Name/IP Address** field to the new name.

Step 5 On the subscriber server, change the name of the subscriber server in Cisco Unified Operating System Administration.

a. From the Settings menu, click **IP > Ethernet**.

b. Change the host name of the publisher server.

c. Click **Save**. The subscriber server automatically restarts.

Step 6 Log on to the publisher server by using an SSH application, and run the CLI command **utils system restart** to restart the server.

Step 7 On the publisher server, run the CLI command **utils dbreplication reset** all to reset replication.

Step 8 Log on to the publisher server by using an SSH application, and run the CLI command **utils system restart** to restart the server a second time.

INDEX

A

C

D

E

H

I

L

M

P

R

S

T

U