



CHAPTER 4

Upgrading from Cisco Unity 4.0(3) or Later with Bridge 3.x

Task List: Upgrading from Cisco Unity 4.0(3) or Later with Bridge 3.x

If you currently have Cisco Unity 4.0(3) or later servers configured for networking with a Bridge 3.x server (or servers), use the task list and procedures in this chapter to upgrade Cisco Unity. Networking with the Octel servers is not disrupted after upgrading Cisco Unity. Therefore, in installations with multiple Cisco Unity servers, you can upgrade the Cisco Unity servers as your schedule permits.

Upgrade the Cisco Unity Bridgehead Server

1. Upgrade the Cisco Unity bridgehead server. For systems using failover, upgrade the secondary server as well. See the “Upgrading Cisco Unity 4.0(x) Software to the Shipping Version” chapter of the applicable *Reconfiguration and Upgrade Guide for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
2. Run ConfigMgr.exe on the Cisco Unity bridgehead server to redesignate it as the bridgehead server. See the “Redesignating the Bridgehead Server” section on page 4-2.

Upgrade Non-Bridgehead Cisco Unity Servers

3. Upgrade all non-bridgehead Cisco Unity servers in the network. For systems using failover, upgrade the secondary servers as well. Networking with the Octel servers is not disrupted after upgrading Cisco Unity. Therefore, in installations with multiple Cisco Unity servers, you can upgrade the Cisco Unity servers as your schedule permits. See the “Upgrading Cisco Unity 4.0(x) Software to the Shipping Version” chapter of the applicable *Reconfiguration and Upgrade Guide for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Optionally, Upgrade the Bridge Servers

If a newer version of the Bridge 3.x software is available, we recommend that you upgrade the Bridge software to the latest version.

4. Upgrade the Bridge server. See the “Upgrading Cisco Unity Bridge 3.x to a Newer Version” section on page 4-2.
5. Install the Cisco Unity Bridge Analog Network and Node Analyzer (BANANA). See the “Installing the Cisco Unity Bridge Analog Network and Node Analyzer (BANANA)” section on page 4-4.

Enable Optional Cisco Unity Features

6. (Optional) If all of the Cisco Unity servers are at version 4.0(4) or later, extend identified subscriber messaging to include Bridge subscribers. See the [“Extending Identified Subscriber Messaging to Include Bridge Subscribers”](#) section on page 4-6.
7. (Optional) If all of the Cisco Unity servers are at version 4.0(4) or later, enable the Bridge server to send delivery receipts to Cisco Unity subscribers when the extended-absence greeting for an Octel subscriber is enabled and the mailbox is accepting messages. See the [“Enabling the Bridge Server to Send Extended-Absence Delivery Receipts”](#) section on page 4-9.
8. Enable the Bridge server to accept requests to push remote mailbox information. See the [“Enabling the Bridge to Accept Requests to Push Mailbox Information”](#) section on page 4-9.

Redesignating the Bridgehead Server

Run the ConfigMgr.exe utility with the Create Bridge Account option to redesignate the server as the bridgehead. (The CsBridgeConnector service will not start, and the Cisco Unity Administrator will not display Bridge-related pages until ConfigMgr.exe has been run.)

To Designate the Bridgehead Server

-
- Step 1** On the Cisco Unity server, browse to the directory in which Cisco Unity is installed (the default location is CommServer).
 - Step 2** Double-click **ConfigMgr.exe**. The ConfigMgr dialog box appears.
 - Step 3** Click **Create Bridge Account**.
 - Step 4** Click **OK** in the dialog box that displays after the configuration has completed.
 - Step 5** Close the ConfigMgr dialog box.
-

Upgrading the Bridge Server

Optionally, upgrade the Bridge server (or servers) to the latest 3.x version.

Upgrading Cisco Unity Bridge 3.x to a Newer Version

We recommend that you upgrade when Bridge message traffic is light. To upgrade to the latest Bridge version from Bridge 3.0(x), do the following procedures in the order presented.

To Disable and Stop Virus-Scanning and Cisco Security Agent Services

-
- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 2** Disable and stop each antivirus service and the Cisco Security Agent service:
 - a. In the right pane, double-click the service.



Note Refer to the antivirus software documentation to determine the names of the antivirus services.

- b. On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
- c. Click **Stop** to stop the service immediately.
- d. Click **OK** to close the Properties dialog box.

Step 3 When the services have been disabled, close the Services MMC.

To Upgrade Cisco Unity Bridge 3.x to a Newer Version

Step 1 Log on to the Bridge server by using the Windows 2000 Server Administrator account.

Step 2 Verify that the account has permission to access the Bridge Administrator.

- a. Open the Bridge Administrator.
- b. If you are allowed access and can view the Bridge Administrator pages, exit the Bridge Administrator and continue with [Step 3](#).



Caution If you are denied access to the Bridge Administrator, do not continue, because the Bridge setup program will fail. You must log off and log back on using another account that is allowed access to the Bridge Administrator. It is possible that the account was denied access to the Bridge Administrator because it is not in the Access Control List of the <Bridge>\Starfish\Asp directory or does not have Full Control permissions to that directory.

Step 3 Open the Services Control Panel on the Bridge server, and stop the following two services:

- Digital Networking
- Unity Bridge

The Bridge services will complete the shutdown process when the last in-process message transmission or reception, rather than call, is complete. No additional message transmissions will begin on the in-process calls—either outbound or inbound—after shutdown has been initiated.

Step 4 If you downloaded the Bridge software from the Software Center website, browse to the directory in which the files were extracted.

If you are using the Cisco Unity Bridge CD, insert the disc in the CD-ROM drive, and browse to the **Install** directory.

Step 5 Double-click **Setup.exe**.

Step 6 Click **Next**.

Step 7 In the Choose Destination Location dialog box, change the installation directory, if applicable, and click **Next**.

Step 8 If a device driver service was previously installed for the Brooktrout voice-fax card, a message asks if you want to overwrite the existing service. Click **Yes** twice.

Step 9 In the Select Country dialog box, select the country for which the voice-fax cards will be configured, and click **Next**.

Step 10 Verify the installation settings, and click **Next**.

- Step 11** When prompted, remove the disc from the CD-ROM drive.
- Step 12** Click **OK** to restart the server.

To Re-Enable and Start Virus Scanning and Cisco Security Agent Services

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 2** Re-enable and start each virus-scanning service and the Cisco Security Agent service:
- In the right pane, double-click the service.



Note Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.

- On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
 - Click **Start** to start the service.
 - Click **OK** to close the Properties dialog box.
- Step 3** When the services have been re-enabled, close the Services MMC.
-

Installing the Cisco Unity Bridge Analog Network and Node Analyzer (BANANA)

BANANA is a stand-alone application that runs on the Bridge server. It is designed to assist with monitoring and troubleshooting analog communication between the Bridge and the Octel nodes in the analog network. It also provides detail and summary information of call activity.



Caution

The drive on which you plan to install BANANA requires at least 1 GB of free disk space.

The following procedures provide details for installing and initiating test calls. See BANANA Help for information about other functionality provided by BANANA.

To Install BANANA

- Step 1** Disable virus scanning services and the Cisco Security Agent service, if applicable.
- Step 2** Insert the Cisco Unity Bridge compact disc in the CD-ROM drive, and browse to the BANANA directory.
- Step 3** Double-click **setup.exe**.
- Step 4** Click **OK** at the welcome screen.
- Step 5** If applicable, change the directory where BANANA will be installed.
- Step 6** Click the **Installation** button.
- Step 7** If applicable, change the program group where BANANA will appear.

- Step 8** Click **Continue**.
- Step 9** If a Version Conflict message box is displayed warning that a file being copied is not newer than the file on your system, click **Yes** to keep the existing file.
- Step 10** When the installation is done, click **OK**.
- Step 11** Enable virus-scanning and the Cisco Security Agent services, if applicable.



Note The most up-to-date version of BANANA is available at <http://www.CiscoUnityTools.com>. When you start BANANA, it checks the CiscoUnityTools website to see if a newer version is available, and if so, prompts you about upgrading.

To Adjust the Message Delivery Window Settings

- Step 1** In the Bridge Administrator, click **Octel Nodes**.
- Step 2** In the Node list, click an Octel node that you want to be tested, and click **Edit**.
- Step 3** On the Octel Node page in the Message Delivery Windows section, adjust the schedule according to following illustration, so that the Bridge will not wait to initiate calls to the Octels to deliver normal, urgent, and administrative messages.

Message Delivery Windows				
Message Type	Enabled	Begin	End	Interval
Normal	<input checked="" type="checkbox"/>	12:00 AM	11:59 PM	1
Urgent	<input checked="" type="checkbox"/>	12:00 AM	11:59 PM	1
Administration	<input checked="" type="checkbox"/>	12:00 AM	11:59 PM	1

Note that BANANA makes only administrative calls when testing the Octel analog network. However, if you adjust the normal and urgent schedules as shown, you do not have to remember to adjust the schedule if you also send test messages from Cisco Unity subscribers to Octel subscribers.

- Step 4** Click **Save**.
- Step 5** Repeat [Step 2](#) through [Step 4](#) for each Octel node that you want to test.

To Initiate Test Calls to the Octel Nodes

- Step 1** On the Bridge server on the Windows Start menu, click **Programs > BANANA > BANANA admin**. The BANANA admin main window displays.
- Step 2** Configure the log and output folder locations.
- Step 3** Specify the Octel nodes to be included when placing test calls.
- Step 4** Place the test calls.
- Step 5** Process the call data, and view the results.

Refer to the BANANA Help for details.

Extending Identified Subscriber Messaging to Include Bridge Subscribers

If all of your Cisco Unity servers are running version 4.0(4) or later, you can extend identified subscriber messaging to include Bridge subscribers.

When a person on a remote voice messaging system who has a corresponding Bridge subscriber account calls a Cisco Unity subscriber and leaves a message, by default Cisco Unity will not identify the message as being from the Bridge subscriber. For Cisco Unity to identify callers whose calling number matches the extension or alternate extension of a Bridge subscriber, identified subscriber messaging (ISM) must be extended to include Bridge subscribers.

See the following sections as applicable to your installation.

- [Installation with Multiple Cisco Unity Servers Networked via Digital Networking, page 4-6](#)
- [Single-Server Installations, page 4-6](#)

Installation with Multiple Cisco Unity Servers Networked via Digital Networking

In installations with multiple Cisco Unity servers networked via Digital Networking, enabling ISM to include Bridge subscribers requires the following:

1. The Cisco Unity servers must be connected to the same phone system or phone system network as described in the “Dialing Domains” section in the “Digital Networking” chapter of the applicable *Networking Guide for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
2. The Cisco Unity servers must be configured to be in the same dialing domain, as described in the “Customizing the Primary Location” section on page 4-7.
3. The automated attendant search scope on each server must be set to the dialing domain as described in the “Setting the Automated Attendant Search Scope” section on page 4-7.
4. Identified subscriber messaging on each server must be enabled as described in the “Enabling Identified Subscriber Messaging” section on page 4-8.
5. Identified subscriber messaging on each server must be extended to include Bridge subscribers as described in the “Extending Identified Subscriber Messaging” section on page 4-8.

Single-Server Installations

In installations with only one Cisco Unity server, enabling ISM to include Bridge subscribers requires the following:

1. The server must be configured with a dialing domain name, as described in the “Customizing the Primary Location” section on page 4-7.

2. Identified subscriber messaging must be enabled as described in the [“Enabling Identified Subscriber Messaging” section on page 4-8](#).
3. Identified subscriber messaging must be enabled for Bridge subscribers as described in the [“Extending Identified Subscriber Messaging” section on page 4-8](#).

Customizing the Primary Location

If your installation consists of multiple Cisco Unity servers networked via Digital Networking, you may have already customized the primary location.

For detailed information about the settings, see the [“Primary Location Profile Settings” section on page 11-1](#).

To Customize the Primary Location

-
- Step 1** In the Cisco Unity Administrator, go to the **Network > Primary Location > Profile** page.
 - Step 2** Enter a meaningful name for the location.
 - Step 3** Enter a Dial ID. The Dial ID identifies this location to Cisco Unity.
 - Step 4** Record a voice name for the location.
 - Step 5** For the Dialing Domain name:
 - If your installation consists of only one Cisco Unity server, and if you plan to enable identified subscriber messaging to include Bridge subscribers, enter a dialing domain name.
 - If your installation consists of multiple Cisco Unity servers networked via Digital Networking, and if this server is integrated with the same phone system as other networked Cisco Unity servers, you may have already added this server to a dialing domain. If not, enter the dialing domain name, or select it from the available list. The list contains names of dialing domain names already configured on at least one other Cisco Unity server in the network.

Note that the dialing domain name is case sensitive and must be entered exactly the same on all of the servers. To ensure that all servers are correctly added to the same dialing domain, enter the dialing domain name on one Cisco Unity server and wait for the name to replicate to the other Cisco Unity servers. By doing so, you also confirm that replication is working correctly among the servers. The time that it takes for the primary location data from other Cisco Unity servers to be reflected on the local server depends on your network configuration and replication schedule.
 - Step 6** Click the **Save** icon.
-

Setting the Automated Attendant Search Scope

If your installation consists of multiple Cisco Unity servers networked via Digital Networking, the auto attendant search scope must be set.

To Set the Automated Attendant Search Scope

-
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
 - Step 3** In the Unity Settings pane, click **Networking—Set Auto Attendant Search Scope**.

- Step 4** In the New Value list, click **1**, and then click **Set** so that Cisco Unity searches for subscribers within the dialing domain.
- Step 5** When prompted, click **OK**.
You do not need to restart Cisco Unity to enable the change.
- Step 6** Click **Exit**.
-

Enabling Identified Subscriber Messaging



Note

If the system is using failover, you must make this change on both the primary and secondary servers because the setting is stored in the registry.

To Enable Identified Subscriber Messaging

- Step 1** In the Cisco Unity Administrator, go to the **System > Configuration Settings** page.
- Step 2** In the Identified Subscriber Messaging section, verify that the **Disable Identified Subscriber Messaging** check box is not checked.
Identified subscriber messaging for subscribers on the same Cisco Unity server is enabled when the check box is unchecked. By default, the box is unchecked.
- Step 3** Click the **Save** icon.
-

Extending Identified Subscriber Messaging

After identified subscriber messaging has been enabled, you must extend it to include Bridge subscribers.

To Extend Identified Messaging

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Networking – Enable Identified Subscriber Messaging (ISM) for AMIS, Bridge, and VPIM Subscribers**.
- Step 4** In the New Value list, click **1**, then click **Set**.
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.
- Step 7** Restart Cisco Unity for the registry setting to take effect.
-

Enabling the Bridge Server to Send Extended-Absence Delivery Receipts

For Cisco Unity subscribers to receive delivery receipts, when the extended-absence greeting for an Octel subscriber is enabled and the mailbox is accepting messages, you need to modify a configuration setting on the Bridge server, as described in the following procedure.

To Enable the Bridge to Send Extended-Absence Delivery Receipts

- Step 1** On the Configuration Menu in the Bridge Administrator, click **Digital Networking**.
 - Step 2** Check the **Enable Extended Absence Notifications** check box.
 - Step 3** Click **Save**.
-

Enabling the Bridge to Accept Requests to Push Mailbox Information

Some remote systems provide the capability to push name information to other nodes. The Bridge provides the capability to accept this mailbox information and use it to update the Bridge directory and the Bridge subscriber directory in Cisco Unity.

By default, the Bridge will reject an attempt by the remote node to push mailbox information (but the call will proceed and the remote node will be able to continue with any additional tasks). When the accept remote push functionality is enabled, the Bridge will accept all administrative name push requests from any remote node, and will process the directory information even if the recorded voice name is not included in the transmission. If the mailbox information sent by the remote node does not match any existing mailbox in the Bridge directory, a new usage-based entry is added to the directory. If the information pertains to a mailbox that already exists in the Bridge directory, the Bridge will modify the directory entry; if the text name is blank or no recorded name is transmitted, the corresponding field will be removed from the directory entry.

Before enabling this feature, you should be familiar with the voice messaging system models, versions, configuration, and subscriber population of each remote node that may push mailbox information to the Bridge. Ensure that any increased call processing and directory activity related to acceptance of non-solicited mailbox information by the Bridge does not delay or block message delivery or result in a larger Bridge subscriber directory than your Cisco Unity and Cisco Unity Bridge deployment was designed to support. Refer to the documentation for the particular model of each remote voice messaging system for additional information on support for and mechanisms used in pushing mailbox information via Octel analog networking.

To Enable the Bridge to Accept Requests to Push Mailbox Information

- Step 1** On the Configuration Menu in the Bridge Administrator, click **System Settings**.
 - Step 2** Check the **Accept Remote Push** check box.
 - Step 3** Click **Save**.
-

