



Maintaining Cisco Unity

Overview: Maintaining Cisco Unity

All of the software and hardware associated with the Cisco Unity server requires maintenance to ensure availability. Degradation in any piece of the installed software can affect server performance. If you do regular maintenance, you can reduce the likelihood of unplanned downtime.

See the following sections in this chapter for more information:

- [Scheduling Maintenance Tasks, page 9-1](#)—This section provides an overview of system maintenance tasks and suggested frequency.
- [Setting Up a Test Environment, page 9-3](#)—This section describes the recommended test and production environments.
- [Configuring Cisco Unity for Maintenance Tasks, page 9-3](#)—This section describes application level maintenance tasks on the Cisco Unity server.
- [Configuring Exchange for Maintenance Tasks, page 9-9](#)—This section describes maintenance tasks for Microsoft Exchange (both on- or off-box configurations) that are related to the maintenance of Cisco Unity.
- [Moving Subscriber Mailboxes, page 9-22](#)—It is possible to move subscribers from one Exchange server to another without having to shut down Cisco Unity.
- [Moving the Unity Messaging System, UAmis, and UOmni Exchange Mailboxes, page 9-25](#)—Like subscriber mailboxes, it is possible to move the Unity Messaging System, UAmis, and UOmni mailboxes from one Exchange server to another, but with a few extra steps to prevent problems that can occur after these special mailboxes are moved.
- [Cisco Unity Failover Feature, page 9-27](#)—This feature provides a redundant Cisco Unity server in the event the primary Cisco Unity server fails, or for use during routine maintenance.
- [Backing Up and Restoring a Cisco Unity System, page 9-27](#)—Backups are essential for restoring Cisco Unity quickly if data is corrupted or lost.

Scheduling Maintenance Tasks

The frequency of scheduled maintenance depends on your particular environment, taking into account such issues as system size, configuration, and traffic levels. At a minimum, we recommend that you do scheduled maintenance as indicated in [Table 9-1](#). If you already do the following tasks more frequently than we recommend, use your schedule rather than our recommendations.

Table 9-1 Maintenance Tasks and How Often to Do Them

Task	Daily	Monthly	Other
Forward unaddressed messages to the appropriate recipients. For more information, see the “Forwarding Unaddressed Messages to the Appropriate Recipients” section on page 9-13.			Continually
Scan for viruses. See the “Scanning for Viruses” section on page 9-12.	X		
Back up the Cisco Unity server. See the “Backing Up and Restoring a Cisco Unity System” section on page 9-27.	X		
Verify that messages in the Unity Messaging Repository (UMR) are being delivered.	X		
Determine if failover has occurred.	X		
Check to see if Cisco Unity Administrator sessions are not in use and are not being freed by Cisco Unity.	X		
Verify that the system back-up is complete before the beginning of the next business day.		X	
Verify that the back-up medium has enough room to back up the entire contents of the Cisco Unity server.		X	
Exchange: Check for Exchange mailboxes that are over their limit. See the “Checking for Mailboxes that Are Over Their Size Limit” section on page 9-15.		X	
Exchange: Schedule the Message Store Manager to do mailbox maintenance tasks, such as deleting old messages and running the Subscriber Message Store Status report. See the “Message Store Manager Utility” section on page 9-5.		X	Or, as necessary, daily or weekly
Install the latest Cisco Unity-qualified service packs and security hot fixes. See the “Installing Service Packs and Updates” section on page 9-15.		X	
Run the Dbwalker Utility to check database integrity. Fix any errors encountered by following the on-screen instructions.		X	
Update the system clock. See the “Updating the System Clock” section on page 9-17.		X	
Exchange 5.5 and Exchange 2000: Free unused space in the Exchange database by using the Eseutil utility. Refer to Article ID 192185, “How to Defragment with the Eseutil Utility,” on the Microsoft website.			Offline defragmentation every six months
Exchange 5.5: Run the Exchange Optimizer. Refer to Article ID 266051, “The ‘Understanding the Microsoft Exchange Server Performance Optimizer’ White Paper Is Available,” on the Microsoft website.			Whenever you add 100 or more Exchange mailboxes or Cisco Unity subscribers

Table 9-1 Maintenance Tasks and How Often to Do Them (continued)

Task	Daily	Monthly	Other
Upgrade third-party software. See the “Upgrading Third-Party Software” section on page 9-15.			As needed
Install new hardware and drivers. See the “Installing New Hardware and Drivers” section on page 9-16.			As needed
Update virus-scanning definitions. See the “Updating Virus-Scanning Definitions” section on page 9-12.			Whenever new definitions become available
Restart the Cisco Unity server. See the “Restarting the Cisco Unity Server” section on page 9-18.			According to your current schedule, or as needed
Run and review Cisco Unity reports.			As needed
Monitor system resources.			According to your current schedule, or as needed
Monitor the available forums for Cisco Unity.			As needed

Setting Up a Test Environment

If your system resources allow it, we recommend establishing a test environment for the entire Cisco Unity deployment. The test environment can be smaller in scale than the production environment, but should have the same configuration characteristics.

Use the test environment to validate any proposed changes prior to implementing them on the production system. This includes any upgrades or patches to Cisco Unity, the phone system, and the network, including but not limited to auto-attendant, ports, schedules, call handlers, class of service and distribution lists, languages, the mail store, and third-party software.

Document both the production and test environment initial configurations, and keep a log of all changes made. Failing to do so can impact the supportability of Cisco Unity in the current environment, causing unnecessary delays if support personnel must work around undocumented changes. Also, failing to document the current environment and any changes made will impact the ability to efficiently and successfully expand the system and to do major upgrades in the future.

Configuring Cisco Unity for Maintenance Tasks

See the following sections:

- [Status Monitor, page 9-4](#)
- [Message Store Manager Utility, page 9-5](#)
- [Event Notification Utility, page 9-6](#)

Status Monitor

The Status Monitor is a Web-based application on the Cisco Unity server that runs separately from the Cisco Unity Administrator. It contains pages that provide information about system status, ports, reports, and disk drives. Each page of the Status Monitor displays key status information from the other Status Monitor pages in the taskbar at the bottom of the screen. (See [Table 9-2](#) for information about each page in the Status Monitor.)

To access the Status Monitor, use one of the following two procedures. The method you use to log on to the Status Monitor depends on which authentication method it uses. Note that the authentication method that you choose to use for the Cisco Unity Administrator automatically applies to the Status Monitor. (To learn more about the authentication methods that you can use with the Cisco Unity Administrator and the Status Monitor, see the [“About Cisco Unity Administrator Authentication”](#) section on page 2-4.)

To Log On to the Status Monitor When It Uses Integrated Windows Authentication






- Step 1** Log on to Windows on the Cisco Unity server (or a remote computer) by using either the administration account or an appropriate Windows domain account.
- Step 2** If you logged on to the Status Monitor on the Cisco Unity server, double-click the desktop shortcut to the Status Monitor.
- If you logged on to the Status Monitor on a computer other than the Cisco Unity server, start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 3** If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or an appropriate Windows domain account.
-

To Log On to the Status Monitor When It Uses Anonymous Authentication

- Step 1** Log on to Windows on the Cisco Unity server (or a remote computer) by using any domain account that has the right to log on locally.
- Step 2** If you logged on to the Status Monitor on the Cisco Unity server, double-click the desktop shortcut to the Status Monitor.
- If you logged on to the Status Monitor on a computer other than the Cisco Unity server, start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 3** On the Cisco Unity Log On page, enter either the user name, password, and domain for the administration account or an appropriate Windows domain account, and click **Log On**.
-

Table 9-2 describes each page in the Status Monitor.

Table 9-2 Status Monitor Pages

Button	Page Name	Description
	System Status	Shows whether Cisco Unity is operating, and allows you to start and exit from Cisco Unity. You can choose to exit after all calls are finished or to interrupt calls in progress with a message and then disconnect all calls and exit.
	Port Status	Shows the status of each port. This page is useful for testing and troubleshooting. For example, you can monitor an incoming call to see which call handlers the call is routed to.
	Report Status	Shows the status of reports that have been generated.
	Disk Drive Status	Shows the total size and the available space of each drive and partition on the Cisco Unity server.
	Help	Displays the online Help.

Access to the Status Monitor is controlled by class of service. Internet Explorer is also required to view the Status Monitor pages.

To Set Up or Modify Access to the Status Monitor

-
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Class of Service** page.
 - Step 2** Click the **Find** icon.
 - Step 3** Double-click the class of service that you want to modify.
 - Step 4** Go to the **System Access** page.
 - Step 5** Check the Unity Administrator Application Access check box.
 - Step 6** Under Troubleshooting and Administration, check the Status Monitor Access check box.
 - Step 7** Click the **Save** icon.
-

Message Store Manager Utility

The Message Store Manager utility, available in Tools Depot, can be used for a variety of subscriber message store maintenance tasks, including reporting message demographics, archiving messages, deleting messages, setting mailstore limits, and hiding mailboxes from the address book, according to configurable schedules.

The Message Store Manager utility allows administrators to set up subscriber groups, called agents. Each action that an administrator does by using the Message Store Manager utility is performed on an agent, or on a specified subset of the members of the agent. Agents are set up by using Cisco Unity distribution lists, classes of service, extension ranges, imported .csv files, or home mail servers, and any membership changes to these groups that are made by using the Cisco Unity Administrator are automatically carried forward to the Message Store Manager agents.

After setting up the agents, configure and schedule the Subscriber Message Store Manager tasks appropriate for each agent to be run daily, weekly, or monthly according to the needs of your site.

One of the maintenance functions of Message Store Manager is the Subscriber Message Store Status report. The Subscriber Message Store Status report is a .csv file that contains detailed data about each subscriber mailbox that was included in the selected agent. It allows administrators to see and have a record of subscriber mailbox information, including the capacity of each mailbox, if mailbox full warnings have been generated, the count and size of all messages in the mailbox, and other information specific to message type.

Subscriber Message Store Status reports are written to a file that is unique to the agent and to the time that the report generation began. For example, the file name for a report for the “Sales” agent could be Sales_MailboxDump_021002_091437.csv. These report files are saved in the Temp folder of the account used to run the report.

For more information on setting up agents and using the Message Store Manager utility, see the online Help for the utility.

Event Notification Utility

The Event Notification utility sends e-mail, voice mail, or both to subscribers or public distribution lists in response to an error condition or potential problem on the Cisco Unity server. The utility monitors the Windows application log and sends notification when a specified event occurs, such as “Disk almost full.” In addition, the utility can also automatically restart the Cisco Unity server when a specified event occurs.

The Event Notification utility has several predefined default event notifications, though some event notifications, such as those which require the Cisco Unity server to automatically restart, are disabled. The notification settings for the default event notifications specify that an e-mail is sent to the System Event Messages distribution list. Because the Example Administrator is by default the only member of this distribution list, assign the appropriate subscriber(s) or public distribution list to the list to ensure that someone receives event notifications. Note that if you later delete the assigned subscribers or distribution lists, Cisco Unity does not prompt you to assign a replacement.

You can disable or enable existing event notifications, as well as modify the event which is monitored, how you are notified when the event occurs, and who receives notification. You can also add new event notifications. There are two types of event notifications that you can create:

Table 9-3 Event Notification Types

Type	Action
NT Event Log	The utility notifies you when a specified application event occurs.
Reboot Cisco Unity	The utility notifies you and automatically restarts Cisco Unity when a specified application event occurs.

Note that Cisco Unity writes events only to the Windows application log; it does not write events to the system or security logs. For information on how to generate an Event Log report for all application events on the Cisco Unity server, or for the events that apply only to Cisco Unity, see the “[Event Log Report](#)” section on page 26-9. You can also view application events by using the Windows Event Viewer (on the Windows Start menu, click Programs > Administrative Tools > Event Viewer). You can identify the Cisco Unity events as those events that begin with CiscoUnity (for example, “CiscoUnity_LogMgr”). For more information on Windows events, refer to the Windows Event Viewer online Help.

To Modify or Add an Event Notification

-
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Reporting Tools, double-click **Event Notification Utility**. The Notification Utility Administration window appears, listing the events monitored by the utility and the type of notification(s) set up for each.
- Step 3** Do one of the following actions, as appropriate:
- To modify an existing event notification, double-click the event that you want to modify. Note that the event notification type is specified in the title bar of the Properties dialog box which appears.
 - To add a new event notification, click **File > New Event**. Then choose the appropriate action:
 - If you want the Event Notification utility to notify you when the event that you specify occurs, click **NT Event Log**.
 - If you want the utility to notify you and automatically restart the Cisco Unity server when the event that you specify occurs, click **Reboot Cisco Unity**.
- Step 4** From the Event tab, do the following actions, as appropriate:
- In the Display Name field, enter the event notification name that you want listed in the Notification Utility Administration window.
 - To enable or disable the event notification, check or uncheck the **Active** check box as appropriate.
 - Select or enter the source, and then enter the event ID of the event that you want the utility to monitor as each is referenced in the Windows application log.
- Step 5** From the Voice Mail Message tab, do one of the following actions, as appropriate:
- To enable or disable voice mail notification, check or uncheck the **Send Message** check box as appropriate.
 - To set up or modify voice mail notification, do the procedure, [To Set Up or Modify Voice Mail Notification, page 9-8](#), and then continue with [Step 6](#) in this procedure.
- Step 6** From the E-Mail Message tab, do the following actions, as appropriate:
- To enable or disable e-mail notification for the event, check or uncheck the **Send Message** check box as appropriate.
 - Complete or modify the remaining fields.
- Step 7** From the SMTP Message tab, do one of the following actions, as appropriate:
- To enable or disable SMTP notification for the event, check or uncheck the **Send Message** check box as appropriate.
 - To set up or modify SMTP notification, do the procedure, [To Set Up or Modify SMTP Message Notification, page 9-8](#), and then continue with [Step 8](#) in this procedure.
- Step 8** Click **OK**.

- Step 9** If necessary, repeat [Step 3](#) through [Step 8](#) to add or modify another event notification.
- Step 10** Click **Tools > Reset Server** to update the utility with your changes. Note that this action resets the Event Notification utility—not the Cisco Unity server. It is not necessary to restart the Cisco Unity server to save your event notification changes.

To Set Up or Modify Voice Mail Notification

- Step 1** Record the message that you want to use as the voice mail message for an event notification by using the Media Master control bar.
- Step 2** Use the Media Master **Copy to File** option to save the recording as a WAV file.
- Step 3** If the Event Notification utility is not already running, on the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Event Notification Utility**.
- Step 4** Go to the Voice Mail Message tab in the Properties dialog box for the appropriate event notification.
- Step 5** Confirm that the Send Message check box is checked, and complete the To and Subject fields.
- Step 6** Enter the directory path where you stored the WAV file that you recorded in [Step 1](#), or click **Browse** to select it.
- Step 7** Complete the remaining fields as appropriate, and then click **OK**.

To Set Up or Modify SMTP Message Notification

You can set up the Event Notification utility to send an e-mail message through an SMTP gateway in response to an error condition or potential problem on the Cisco Unity server. This capability is useful when Exchange has gone down, or if you want to send notification through the Internet to an e-mail address at another location.

- Step 1** If the Event Notification utility is not already running, on the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Event Notification Utility**.
- Step 2** Go to the SMTP Message tab in the Properties dialog box for the appropriate event notification.
- Step 3** Confirm that the **Send Message** check box is checked.
- Step 4** In the SMTP Server field, enter either the IP address or the fully-qualified domain name of an SMTP server that is not on your Exchange network.
- Step 5** In the Port field, confirm that the port number for the SMTP server is correct for your site. Consult your network administrator for more information.
- Step 6** Complete the From field as appropriate. You can enter a name or an e-mail address.
- Step 7** In the To field, enter the e-mail address of the message recipient.
- Step 8** Complete the remaining fields as appropriate, and then click **OK**.

Monitoring Cisco Unity Performance

Refer to the *White Paper: Monitoring Cisco Unity Performance*, available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_technical_reference_list.html.

Configuring Exchange for Maintenance Tasks

On any Exchange server that is the home server for Cisco Unity subscribers, do the tasks in the following sections:

- [Setting a Maximum Size for Exchange Mailboxes](#), page 9-9
- [Circular Logging in Exchange](#), page 9-10
- [Monitoring the Message Transfer Agent](#), page 9-12

Existing Microsoft best practices can be researched and utilized based on system scaling and traffic patterns. Refer to the Microsoft website for best practices on maintaining Microsoft products.

Setting a Maximum Size for Exchange Mailboxes

Voice messages can consume significant amounts of disk space. For example, voice messages recorded by using the G.711 codec consume 480 KB/minute. If all Cisco Unity subscribers save every voice message they receive, the hard disk where messages are stored can quickly run out of space. To prevent this from happening, set limits on the size of subscriber Exchange mailboxes.

To view and set the size of subscriber mailboxes, you can use the Message Store Manager utility, available in Tools Depot (see the “[Installing Service Packs and Updates](#)” section on page 9-15.) Or, if you prefer, use the following procedures for Exchange 2000 or Exchange 5.5.

For more information on Exchange 5.5 and Exchange 2000 storage limits, refer to the Microsoft Exchange documentation. You can also review the *White Paper: Understanding How Exchange 2000 Storage Limits Work with Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_technical_reference_list.html.

To learn more about how Cisco Unity handles subscribers with full mailboxes, see the “[How Cisco Unity Handles Subscribers Whose Mailboxes Are Full](#)” section on page 5-2.

Exchange 2000

To Set Limits for all Users in Exchange 2000

- Step 1** On the Windows Start menu, click **Programs > Microsoft Exchange > System Manager**.
 - Step 2** In the left pane, expand **Servers**, expand the appropriate server, and expand the storage group.
 - Step 3** Right-click **Mailbox Store**, and click **Properties**.
 - Step 4** Click the **Limits** tab.
 - Step 5** In the Storage Limits section, specify values as appropriate.
-

If you want to set different limits for individual users (for example, set no limit for the company president), do the following procedure.

To Set Limits for Individual Users in Exchange 2000

- Step 1** On the Windows Start menu, click **Programs > Microsoft Exchange > Active Directory Users and Computers**.

- Step 2** In the left pane, expand the server.
 - Step 3** In the left pane, click the folder in which the user appears (by default, the folder is named Users).
 - Step 4** In the right pane, right-click the user name, and click **Properties**.
 - Step 5** Click the **Exchange General** tab.
 - Step 6** Click **Storage Limits**.
 - Step 7** In the Storage Limits dialog box, uncheck the **Use Mailbox Store Defaults** check box.
 - Step 8** Specify values as appropriate.
-

Exchange 5.5

To Set Limits for all Users in Exchange 5.5

- Step 1** On the Windows Start menu, click **Programs > Microsoft Exchange > Microsoft Exchange Administrator**.
 - Step 2** In the left pane, expand the site, expand **Configuration**, expand **Servers**, and expand the appropriate server name.
 - Step 3** In the left pane, click **Private Information Store**.
 - Step 4** On the Exchange Administrator menu, click **File > Properties**.
 - Step 5** On the General tab, specify values in the Storage Limits section as appropriate.
-

If you want to set different limits for individual users (for example, set no limit for the company president), do the following procedure.

To Set Limits for Individual Users in Exchange 5.5

- Step 1** On the Windows Start menu, click **Programs > Microsoft Exchange > Microsoft Exchange Administrator**.
 - Step 2** In the left pane, expand the site and click **Recipients**.
 - Step 3** In the right pane, double-click the mailbox whose limit you want to change.
 - Step 4** Click the **Limits** tab.
 - Step 5** In the Use Information Store Defaults section, uncheck the **Use Information Store Defaults** check box.
 - Step 6** Specify values as appropriate.
-

Circular Logging in Exchange

You can configure logging in one of two ways: either the existing logs are overwritten when hard disk space runs low, or the existing logs are never overwritten. Turn on circular logging if you want to do full backups every time you back up the system. Otherwise, turn it off to have more flexibility with your backup schedule.

Exchange 5.5 and Exchange 2000 store data in Jet databases. The most current transactions are stored in the Edb.log file. When the Edb.lg file reaches 5 MB in size, Exchange checks to see if the oldest transactions in the file have been committed to the database. If they have, then the old transactions are overwritten with new transactions, preventing the total size of the log files from growing beyond 25 to 30 MB in size. Exchange will not, however, overwrite any transactions that have not been committed to the database. This process is referred to as circular logging. When circular logging is enabled, full backups of Exchange are always required.

When circular logging is disabled, and the Edb.lg file reaches 5 MB in size, Exchange creates a new log file of the same name, and renames the inactive file. The number of log files increases as more transactions are logged, and the system continues to create new log files until a backup is completed. If you disable circular logging, we recommend that you set a backup schedule to do full backups periodically, and incremental backups at all other times.

After you back up the message store by using Exchange-aware backup software, the backup software clears the transaction logs. At this point, the backup reflects the current state of the message store, so the transaction logs are no longer required to restore the message store.

**Caution**

If circular logging is enabled and hard disk space runs low, the newest transaction log entries (which contain the newest messages) overwrite the oldest log entries (the oldest messages). When log entries are overwritten, you cannot use the transaction logs to restore messages that were received after the last backup. If disk space is very low and if the system is very busy, old entries may be overwritten in less than a day.

If you decide to disable circular logging, confirm that scheduled incremental and full backups continue to run and that they do not fail or stop working for any reason. If backups are not done, the transaction logs can cause the hard disk to fill up, which in turn causes Exchange to stop working, and subsequently can cause Cisco Unity to stop working.

We strongly recommend that you do the following:

- Use Exchange-aware backup software to back up the message store.
- Carefully watch the amount of available space on the hard disk or in the partition where logs are stored, and free up disk space when the amount of available space gets too low.

To Turn Circular Logging Off for Exchange 5.5

- Step 1** In the left pane of Microsoft Exchange Administrator, select the server.
- Step 2** On the Exchange Administrator File menu, click **Properties**.
- Step 3** Click the **Advanced** tab.
- Step 4** In the Database Circular Logging section, uncheck the **Information Store** check box.

If you also want to turn circular logging off for the directory, you can also uncheck the **Directory** check box.

Monitoring the Message Transfer Agent

Monitor the MTA (UnityMTA and UnityMTA\failed folders) to confirm that messages are going to the appropriate subscriber home servers. The MTA queue can contain messages that did not go to subscriber home servers if there has been a loss of network connectivity, if the Exchange server has gone off-line, or if there is a DNS issue (if the name of either the sending or home server cannot be resolved, the messages cannot be sent to the home server.)

For Exchange 5.5 systems, refer to Microsoft Knowledge Base article 247133, available on the Microsoft support website, for additional information.

Monitoring System Resources

Monitor for low free disk space on all hard disks and partitions on the Cisco Unity server. What constitutes low disk space can vary from partition to partition. For the operating system partition, 10 percent available disk space may suffice. For the data store, 25 percent or less of available disk space should generate a notification to the system administrator.

The Cisco Unity Performance Information and Diagnostics utility, available in Tools Depot, provides logging of performance data to a .csv file.

Scanning for Viruses

Selecting Virus-Scanning Software

For a list of the virus-scanning software that has been qualified for use with Cisco Unity, refer to the System Requirements document for your version of Cisco Unity, available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.

Scheduling Virus Scanning

Schedule virus scanning to occur daily. Ideally, virus scanning should occur when the server is least busy so that it does not interfere with Cisco Unity voice messaging functions.

Updating Virus-Scanning Definitions

Your virus-scanning software should be configured to alert you every week or two to check the manufacturer website for new virus-scanning definitions. If you already have a policy for updating these definitions on the other computers on your network, follow the same policy for the Cisco Unity server. If you do not already have a policy, download and install the new definitions on the Cisco Unity server whenever the software prompts you to do so.

Managing the Location of Log Files and Database Files

The way in which logical drives on the Cisco Unity server are partitioned and what content is located on the drives depends on the size of the Cisco Unity system, the RAID volume configuration used, whether the system will be installed as Voice Messaging Only (VM) or as Unified Messaging (UM), and whether Exchange is used on-box or off-box.

The partition and drive content recommendations from the *Cisco Unity Installation Guide* should continue to be followed when maintaining your system.

For more information on storage issues, refer to *White Paper: Physical Storage Best Practices for Cisco Unity with Microsoft Exchange*, available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_technical_reference_list.html.

Performing Scheduled Maintenance on the Cisco Unity Server

See the following sections for detailed information on scheduled maintenance tasks:

- [Forwarding Unaddressed Messages to the Appropriate Recipients, page 9-13](#)
- [Checking for Mailboxes that Are Over Their Size Limit, page 9-15](#)
- [Installing Service Packs and Updates, page 9-15](#)
- [Installing New Hardware and Drivers, page 9-16](#)
- [Updating the System Clock, page 9-17](#)
- [Restarting the Cisco Unity Server, page 9-18](#)

Forwarding Unaddressed Messages to the Appropriate Recipients

In some situations, messages left in Cisco Unity are not associated with a specific recipient, and therefore they must be screened and routed to the appropriate subscriber or call handler. A subscriber should be assigned the responsibility of reviewing these messages frequently, and forwarding them to the appropriate recipient(s). See the procedure below for instructions on adding subscribers to the applicable distribution list(s).

To Add Subscribers to the Unaddressed Messages or System Event Messages Distribution Lists

-
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.
 - Step 2** Click the **Find** icon.
 - Step 3** Double-click the **Unaddressed Messages** or **System Events Messages** distribution list.
 - Step 4** Change settings as appropriate, and then click the **Save** icon.
-

Unaddressed Messages Distribution List

Messages that cannot be delivered because the network or a server assigned to a subscriber has gone off-line or is otherwise unavailable to the Cisco Unity server, or because the subscriber mailbox has exceeded the Prohibit Send and Receive limit specified for the mailbox in Exchange, are forwarded to the Unaddressed Messages distribution list. By default, this distribution list contains the Example Administrator as its only member.

To route these messages properly, verify that the Unaddressed Messages distribution list has at least one member (such as the operator) who will monitor the mailbox and handle messages that cannot be delivered. To add subscribers to the distribution list, do the procedure, [“To Add Subscribers to the Unaddressed Messages or System Event Messages Distribution Lists”](#) section on page 9-13. (For information about public distribution lists, see the [“Overview: Public Distribution Lists”](#) section on page 18-1.)

Note that if the mailbox(es) of the subscriber(s) who are assigned to check the Unaddressed Messages list exceed the Prohibit Send and Receive storage limit that is specified in Exchange, any messages sent to the Unaddressed Messages distribution list are lost. To avoid this problem, specify a generous value for the Prohibit Send and Receive storage limit for the mailbox of at least one subscriber who is a member of the Unaddressed Messages list, and encourage the subscriber to dispose of messages promptly so that the Exchange mailbox does not fill up. (To learn more about how Cisco Unity handles subscribers with full mailboxes, see the [“How Cisco Unity Handles Subscribers Whose Mailboxes Are Full”](#) section on page 5-2.)

System Event Messages Distribution List

Messages sent from the Event Notification utility are forwarded to the System Event Messages distribution list. By default, this distribution list contains the Example Administrator as its only member. To route these messages properly, add a subscriber (such as the operator) to the System Event Messages distribution list.

Operator, Opening Greeting, and Goodbye Call Handlers

When a caller to Cisco Unity dials the operator and no operator is available, the caller can leave a message, depending on the call transfer settings for the Operator call handler. Call transfer settings in the Opening Greeting and Goodbye call handlers also can allow callers to leave a message. By default, messages left in any of these call handlers are sent to the Unaddressed Messages distribution list. For more information on call handler message recipient settings, see the [“Call Handler Messages Settings”](#) section on page 21-13.

Example Interview

When callers are routed to the Example Interview, which gathers basic information about who they are and who they are trying to reach, the answers to the questions are routed by default to the Example Administrator. If you want the Example Interview messages to be routed to another recipient, choose a subscriber (such as the operator) or a distribution list as the recipient. For information on choosing an interview response recipient, see the [“Overview: Interview Handler Settings”](#) section on page 23-1.

Checking for Mailboxes that Are Over Their Size Limit

If you set limits on the maximum size of subscriber mailboxes as recommended in the “[Setting a Maximum Size for Exchange Mailboxes](#)” section on page 9-9, run the Subscriber Message Store Status report as described in the “[Message Store Manager Utility](#)” section on page 9-5. To learn more about how Cisco Unity handles subscribers with full mailboxes, see the “[How Cisco Unity Handles Subscribers Whose Mailboxes Are Full](#)” section on page 5-2.

Installing Service Packs and Updates

Microsoft updates (referred to by a variety of names, including security updates, critical updates, patches, and hot fixes) are limited to changes that fix specific problems. They do not include general defect fixes or new functionality. All of these Microsoft updates are qualified by Cisco from the day that Microsoft releases them. Cisco recommends that these Microsoft updates be applied to the Cisco Unity server as they are released. Cisco TAC provides support for a Cisco Unity system on which such updates have been installed.

Microsoft also occasionally releases service packs that contain fixes generated since the general product release, including most fixes that were released as updates.

Because the service pack scope is broad, each service pack must be thoroughly tested to ensure that changes do not adversely affect Cisco Unity. Cisco TAC does not support new service packs until they have been qualified for use with Cisco Unity. Do not install a service pack or maintenance release that has not been qualified, or Cisco TAC will not help you resolve problems until you uninstall it.

For the most current information on which Microsoft service packs have been qualified for use with Cisco Unity, refer to *Compatibility Matrix: Required and Recommended Third-Party Service Packs*, available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.

Upgrading Third-Party Software

Cisco support policy is that customers can deploy third-party software for backup, monitoring, and security on the Cisco Unity server. However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with Cisco Unity before the products are deployed, to mitigate the risk of problems being discovered within the production environment between Cisco Unity and the third-party products loaded on the Cisco Unity server.

If a customer calls Cisco TAC with a problem, a Cisco TAC engineer may require that such third-party software be turned off or even removed from the Cisco Unity server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and Cisco Unity was the root cause of the problem, then the third-party software will be required to be disabled or removed from the Cisco Unity server until such time that the interoperability issue is addressed, so that the customer can continue to have a functional Cisco Unity system.

Before installing any qualified Microsoft service pack on the Cisco Unity server, confirm that the manufacturer of any optional third-party software or hardware that you plan to install on the Cisco Unity server—or that is already installed—also supports the service pack for use with its product.

For information on third-party software that has been qualified for use with Cisco Unity, refer to *Cisco Unity System Requirements, and Supported Hardware and Software*, available on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html.

Installing New Hardware and Drivers

Cisco Unity servers that you purchase from Cisco Systems are configured for a specific hardware setup. Do not add or change any hardware on the server, other than to add voice cards, processor(s), memory, a tape drive, an external modem, or a rail kit.

Running the DbWalker Utility

The DbWalker utility checks each call handler, subscriber, subscriber template, interview handler, location object, and directory object in the Cisco Unity database for missing values, broken links, and other problems. Dbwalker must be run on the Cisco Unity server. It can not be run off-box.

The utility runs in two modes: scheduled and manual. Scheduled mode is a read-only review of the database. Manual mode can make automatic database repairs using site-specific information.

Both scheduled and manual modes create an output log file. The log file lists any errors found, shows automatic repairs of missing values and broken links, and also gives advisory warning messages for any items that require investigation and that may require a manual repair. The log file can be sent to a system manager or designated subscriber via e-mail, provided that the site security configuration allows this. The DbWalker utility also offers a choice for log file output content. We recommend that only the errors and warnings are reported, not a complete list of the entire database, due to the potential for a very large output file.

Schedule the DbWalker utility to run (in read-only mode) monthly. Following each monthly scheduled run, two tasks are required of the system manager or their designee for database maintenance:

- Review the output log file.
- Promptly resolve any errors or missing information. Run the DbWalker utility a second time in manual mode using site-specific information to make database repairs, then fix any remaining problems noted in the log by using the Cisco Unity Administrator.

To Schedule the DbWalker Utility to Run Monthly (Read-Only)

- Step 1** On the Cisco Unity desktop, confirm that Cisco Unity is running, then double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Diagnostic Tools, double-click **DbWalker**.
- Step 3** On the Directory Walker page, in the Options list, confirm that no check boxes are checked.
- Step 4** In the Logging section, enter the location of your choice for the output log files.
- Step 5** Choose a Logging Detail method. We recommend you choose **Log Only Information About Objects with One or More Errors**.
- Step 6** To send the monthly output log file to the system manager or to a designated subscriber, click **Schedule > E-Mail Notification**.
- Step 7** Enter a valid subscriber e-mail address, then click **Send Test Message**.
- Step 8** Verify that the test e-mail message was received. Note that firewalls and other site security measures may prevent e-mail message receipt.
- Step 9** Click **Save**.
- Step 10** On the Directory Walker page, click **Schedule > Schedule DbWalker to Run**.
- Step 11** In the DbWalker Scheduler window, click **Schedule Walk**.

- Step 12** Click **OK** to accept the default task name, or enter the task name of your choice. To change an existing schedule, click **Task Properties**.
 - Step 13** In the DbWalker window, on the Tasks tab, check the **Enabled** check box, and complete the remaining fields as needed for your site.
 - Step 14** Click the Schedule tab, choose **Schedule Tasks Monthly**, and complete the remaining fields as needed for your site.
 - Step 15** Click the Settings tab, and complete the fields as needed for your site.
 - Step 16** Click **Apply**, then click **OK**, then click **Close**. The DbWalker utility will run as scheduled.
 - Step 17** When the DbWalker utility has run, review the DbWalker output log file. Investigate all errors and warning messages. Resolve any missing or incorrect information in the database by doing the following procedure and by using the Cisco Unity Administrator.
-

To Run the DbWalker Utility Manually (With Database Repairs)

- Step 1** On the Cisco Unity desktop, confirm that Cisco Unity is running, then double-click the **Cisco Unity Tools Depot** icon.
 - Step 2** In the left pane, under Diagnostic Tools, double-click **DbWalker**.
 - Step 3** In the Options list, select the automatic repairs that you want the utility to perform.
 - Step 4** In the Logging section, confirm the location and the Logging Detail method for the output log file. We recommend you choose **Log Only Information About Objects with One or More Errors**.
 - Step 5** Click **Walk Database**. The DbWalker utility will run and any automatic repairs selected will be performed.
 - Step 6** When the DbWalker utility has run, review the output log file. Investigate all errors and warning messages. Resolve any missing or incorrect information in the database by using the Cisco Unity Administrator.
-

Updating the System Clock

When the Cisco Unity server is connected to the network, we recommend that you configure an authoritative time server to ensure that all computers in the organization use a common time. Refer to Article ID 216734, “How to Configure an Authoritative Time Server in Windows 2000,” on the Microsoft support website.

When the system clock on the Cisco Unity server is slow by a significant amount, subscribers may believe that Cisco Unity is delaying message delivery.

If the Cisco Unity server is not connected to the network, check the system clock monthly to ensure that the time is accurate to within a minute. To change the time, use the Date/Time Control Panel (on the Windows Start menu, click Settings > Control Panel > Date/Time).

Do not change the time on the system clock while you are using the Cisco Unity Administrator, or you may encounter inconsistencies in the data. This is due to an IIS caching problem. The new values have been written to the SQL Server database, but the old values still appear in the IIS cache, so the Cisco Unity Administrator seems to show that you have not changed values that you did change.

Restarting the Cisco Unity Server

Depending on how your network is configured, Cisco Unity services may rely on the availability of a number of other servers on the network, as follows:

- The server that homes the Unity System mailbox
- The server(s) that home Cisco Unity subscriber mailboxes
- Exchange partner servers
- The domain controller for the domain in which the Cisco Unity server belongs
- The Active Directory global catalog server
- The Cisco CallManager server (if Cisco Unity is integrated with Cisco CallManager)
- The Cisco Unity secondary server, when Cisco Unity is configured for failover
- The Exchange 2000 Voice Connector server

The availability of each of these servers, the network connection to these servers, and the corresponding components on the Cisco Unity server may each affect Cisco Unity services.

When you restart servers or network devices on your regular schedule, include Cisco Unity servers in this schedule.

The Unity Schedule Restart tool, available in Tools Depot, allows you schedule an automatic restart of the Cisco Unity server (recommended), or just the Cisco Unity services. You can also use the tool to view Application Event log entries related to restarting Cisco Unity.

To Schedule Cisco Unity Restarts

To change an existing schedule, delete the task and schedule a new task, as shown in the following steps.

-
- Step 1** On the Cisco Unity desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 2** In the left pane, under Administrative Tools, double-click **Schedule Unity Restart**.
 - Step 3** In the Configure Scheduled Restart Options window, choose to restart the Cisco Unity server (recommended), or to restart Cisco Unity services only.
 - Step 4** Click **Schedule Restart**, and complete the fields as needed for your site.
 - Step 5** Click **Save and Exit**.
-

Accessing Cisco Unity Remotely

There are several methods that allow remote access to the Cisco Unity server so that you can do tasks—such as loading updates or patches, and transferring files—that otherwise would have to be done locally. Depending on your site, you can set up remote access to the Cisco Unity server by using:

- Windows Terminal Services—See the [“Using Windows Terminal Services”](#) section on page 9-19.
- Symantec pcAnywhere—See the [“Using pcAnywhere”](#) section on page 9-20.
- A Virtual Private Network (VPN)—See the [“Using a Virtual Private Network”](#) section on page 9-22.

Using Windows Terminal Services

Windows Terminal Services (WTS) comes with Windows 2000, and should already be set up on the Cisco Unity server. In order to set up and use WTS on your remote computer, do the following procedures. (For details on setting up WTS on the Cisco Unity server, refer to the *Cisco Unity Installation Guide*.)

To find additional information about WTS, refer to the online Help available from either the Terminal Services server program on the Cisco Unity server, or from the Terminal Services Client program that you install on the remote computer. You can also refer to the Microsoft website.

To Create the Windows Terminal Client Install Disks

To use WTS on a remote computer, you must first create a set of install disks by using the WTS host program on the Cisco Unity server. You will need two blank disks—labeled “Disk 1” and “Disk 2”—to do this procedure.

-
- Step 1** On the Cisco Unity server, click **Start > Programs > Administrative Tools > Terminal Services Client Creator**.
- Step 2** In the Create Installation Disk(s) dialog box, do the following:
- Click **Terminal Services for 32-bit x86 Windows**.
 - Check the **Format Disk(s)** check box to erase any existing data on the disks, and then click **OK**.
- Step 3** Follow the on-screen instructions to create the two install disks.
- Step 4** Close the **Create Installation Disk(s)** dialog box.
-

To Set Up the WTS Client on a Remote Computer

-
- Step 1** On the remote computer, insert Disk 1 in the A drive, and run **setup.exe**.
- Step 2** Follow the on-screen instructions to complete the installation.
- Step 3** On the Windows Start menu, click **Programs > Terminal Services Client > Client Connection Manager**.
- Step 4** In the Client Connection Manager window, click **File > New Connection**.
- Step 5** Follow the on-screen instructions to complete the Connection Wizard.
-

To Start a Remote Session with WTS

When you connect to the Cisco Unity server from a remote computer by using WTS, your computer controls the server. The Cisco Unity server screen appears within a window on your remote computer and, in general, you can access any of the server files and applications. It is recommended that the Cisco Unity server host only one WTS connection at a time.

-
- Step 1** On the remote computer, do one of the following:
- In the Client Connection Manager window, double-click the new connection icon that was created in the previous procedure.

- On the Start menu, click **Programs > Terminal Services Client > <new connection icon>**. If you changed the default location for the new connection icon, go to the location that you specified in the previous procedure.

Step 2 Log on to the Cisco Unity Administrator with the appropriate name and password.

To Do File Transfers

Step 1 On the remote computer, run `\\<IP Address for Cisco Unity Server>\c$`.

Step 2 Log on to the Cisco Unity Administrator with the appropriate name and password.

Step 3 Transfer files by using either copy-and-paste or drag-and-drop Windows commands.

To End a Remote Session with Windows Terminal Services

Step 1 On the remote computer, log off and exit the Cisco Unity Administrator.

Step 2 Close the **Terminal Services Client <New Connection>** window.

Step 3 When prompted, click **OK** to end the remote connection session.

Windows Terminal Services Limitations

WTS is supported in the following cases:

- For use on a Cisco Unity Bridge server, version 2.0(1) and later
- For use on a Cisco Unity server, version 4.0(1) and later (with limitations as shown in [Table 9-4](#))

Table 9-4 Windows Terminal Services Limitations with Cisco Unity

Remote Functionality	Cisco Unity 4.0(1) and Later
Install or upgrade Cisco Unity	Not supported
Set the dB level of recorded names and greetings by using the Set Volume utility	Not supported
Convert recorded names and greetings to a different codec by using the Set Wav Format utility	Not supported

Using pcAnywhere

You can install pcAnywhere on the Cisco Unity server and on remote computer(s) that will be used to access the Cisco Unity server in your organization. Contact your reseller for the appropriate number of licenses.

Use the following procedures to set up and use pcAnywhere on a remote computer. For more detailed procedures or information about the other pcAnywhere capabilities that may be useful to you, refer to the pcAnywhere documentation.

To Set Up pcAnywhere on a Remote Computer

- Step 1** Insert the pcAnywhere compact disc in the remote computer.
- Step 2** Follow the on-screen instructions to complete the installation.
- Step 3** On the Windows Start menu, click **Programs > Symantec pcAnywhere**, or double-click the desktop shortcut provided.
- Step 4** In the pcAnywhere Manager window, double-click the **Add Remote** icon.
- Step 5** From the Connection Info tab, do the appropriate action:
- If you are using a modem connection, check the appropriate check box in the Device List to indicate the modem that is used by your remote computer. Then, click the **Settings** tab, and enter the phone number of the Cisco Unity server in the Use Dialing Properties and Phone Number fields.
 - If you are using a LAN connection, confirm that **TCP/IP** is selected. Then, click the **Settings** tab, and enter the IP address for the Cisco Unity server in the Network Host PC to Control or IP Address field.
- Step 6** If desired, enter or change other properties as needed on the remaining tabs.
- Step 7** Click **OK**.
- Step 8** Enter a name for the new Remote icon that you just created, and then press **Enter**.
-

To Start a Remote Session with pcAnywhere

When you connect to the Cisco Unity server from a remote computer by using pcAnywhere, your computer controls the server. The Cisco Unity server screen appears within a window on your remote computer and, in general, you can access any of the server files and applications. Before you start a remote session, confirm that pcAnywhere is running in host mode on the Cisco Unity server. If you plan to use a modem connection, confirm that there is no checkmark in the Launch With Windows check box on the Settings tab of the Host Properties dialog box.

Note that a Cisco Unity server can host only one pcAnywhere connection at a time.

- Step 1** On the remote computer, double-click the desktop shortcut provided to start pcAnywhere.
- Step 2** Double-click the new Remote icon that was created in the previous procedure.
- Step 3** When it becomes available, click the listing for the Cisco Unity server that you want to access, and then click **OK**.
- When a connection with the Cisco Unity server is established, the desktop of the Cisco Unity server appears, and the pcAnywhere online toolbar is displayed across the top of the screen.
- Step 4** If desired, do the following actions to improve your connection speed:
- a. From the pcAnywhere online toolbar, click **View/Modify Online Options**.
 - b. In the Online Options dialog box, click **16 Colors** from the Color Scale menu, and then click **OK**.
- Step 5** Log on to the Cisco Unity Administrator with the appropriate name and password.
-

To End a Remote Session with pcAnywhere

- Step 1** On the remote computer, log off and exit the Cisco Unity Administrator.
-

Step 2 From the pcAnywhere online toolbar, click **End Remote Control Session**, and then click **Yes**.

Using a Virtual Private Network

A Virtual Private Network (VPN) is a private network that uses public phone lines (or in some cases a cable modem). Privacy is maintained through encryption and the use of secure protocols. When you use a VPN to access Cisco Unity through a firewall, you will be able to use Cisco Unity as if you were inside the network.

VPN is required if you need to:

- Access the Cisco Unity Administrator website (<http://<Cisco Unity server name>/web/sa>) from a remote computer outside your network firewall.
- Utilize the Media Master control bar to record voice names and greetings by using Distributed Component Object Model (DCOM) to connect your remote computer to the Cisco Unity server through a firewall.



Note If you are not using VPN for remote access, refer to the Microsoft website for information on configuring DCOM through a firewall.

Discuss setting up a VPN with your LAN administrator.

Moving Subscriber Mailboxes

From time to time you may need to move subscriber mailboxes to another server that is faster or has more disk space available, or you may want to move mailboxes when you add new servers to your network. It is possible to move subscribers between servers without having to shut down Cisco Unity.



Caution

If you are moving a group of subscriber mailboxes at once, confirm that you do not inadvertently select the Unity Messaging System, UAmis, or UOmni mailboxes. To move these special mailboxes, see [“Moving the Unity Messaging System, UAmis, and UOmni Exchange Mailboxes” section on page 9-25](#).

If your Cisco Unity server is connected to Exchange 2000, follow the instructions in the Microsoft Exchange documentation to move mailboxes from one server to another. However, if your Cisco Unity server is connected to Exchange 5.5, you need to use the Bulk Logout utility to direct the Cisco Unity server(s) to log out of the mailboxes that you plan to move before you move them in Exchange. With the Bulk Logout utility, you can select the subscriber mailboxes that you want to log out of Exchange 5.5 on each Cisco Unity server in your site. You can select one or more of the following:

- All subscriber mailboxes.
- A group of subscriber mailboxes, based on an extension range, membership in a public distribution list, an association with a class of service (COS), or an assigned phone system (in dual phone system environments).
- You can also use a comma-separated value (CSV) file to select subscribers based on their Exchange aliases. CSV is a common text file format for moving data from one data store to another. You can edit CSV files in a text editor or in a spreadsheet application. If you choose to select subscribers from a CSV file, format your file by using the following guidelines to ensure that it parses correctly:

- Separate values by commas. Do not use a tab, spaces, or a semicolon to separate values in the file.
- Include a column header titled “alias” in the first line. Column headers are not case sensitive, and can be formatted with spaces on the left, right, or on both sides.

For example:

```
first name, last name, home server, alias, domain
Alex, Abade, EXServer1, aabade, ENG_MAIN
Kelly, Bader, EXServer1, kbader, ENG_MAIN
```

To move multiple subscriber mailboxes between Exchange 5.5 servers while Cisco Unity is running, do the appropriate procedures that follow, in the order listed. Note that if your Cisco Unity server is connected to Exchange 2000, you do not need to do these procedures. Instead, you can move Exchange 2000 mailboxes by following the instructions in the Microsoft Exchange documentation.

To Force Cisco Unity to Log Out of Multiple Exchange 5.5 Mailboxes

Step 1 Confirm that subscribers have exited Outlook and have logged off of Cisco Unity.



Caution

The mailboxes that you plan to move must not be accessed until after they have been moved and the Exchange directory has replicated. Subscribers must understand not to start Outlook or to access Cisco Unity over the phone until notified by you that it is okay to do so. If mailboxes are accessed during this process, subscribers will be disconnected, and the Cisco Unity server may need to be restarted.

Step 2 Start the Bulk Logout utility, available in Tools Depot, and then run it on the drive on which Cisco Unity is installed.

Step 3 In the Bulk Subscriber Logout window, select the subscribers that you want to log out of Exchange by doing one of the following:

- Click **All Subscribers**.
- Click **Subscribers with Extension Numbers**, and then enter the range in the From and To fields.
- Click **All Subscribers in this Public Distribution List**, and then click the distribution list from the list in the adjacent field.
- Click **All Subscribers Associated with this Class of Service**, and then click the COS from the list in the adjacent field.
- Click **All Subscribers with Aliases in this CSV File**, and then click **Browse** to locate the CSV file.

Step 4 Click **Add Subscribers to Grid**. The subscribers that you selected in [Step 3](#) are displayed in the grid. If you selected subscribers from a CSV file, note that only those subscribers with mailboxes associated with the local Cisco Unity server are displayed.

Step 5 Repeat [Step 3](#) and [Step 4](#), if appropriate, to add additional subscribers to the grid.

Step 6 If necessary, check or uncheck the check boxes next to each subscriber listed in the grid to add or remove subscribers from the group that you selected for log out.

Step 7 Click **Log Out Subscribers**, and follow the on-screen instructions. For the selected subscribers, Cisco Unity logs out of all Exchange mailboxes that are associated with the local Cisco Unity server.

Step 8 If subscribers are associated with more than Cisco Unity server, or if you are not sure which Exchange mailboxes are associated with which Cisco Unity servers in your site, repeat [Step 2](#) through [Step 7](#) for each Cisco Unity server in your site as necessary.

- Step 9** Leave the Bulk Subscriber Logout window open, and continue with the following procedure.
-

To Move Exchange 5.5 Mailboxes

- Step 1** On the Windows Start menu, click **Programs > Microsoft Exchange > Microsoft Exchange Administrator**.
- Step 2** In the tree in the left pane, click **Recipients**, then click the name(s) of the subscriber(s) in the right pane.



Caution If you are moving a group of subscriber mailboxes at once, confirm that you do not inadvertently select the Unity Messaging System, UAmis, or UOmni mailboxes. To move these special mailboxes, see [“Moving the Unity Messaging System, UAmis, and UOmni Exchange Mailboxes”](#) section on page 9-25.

- Step 3** Click **Tools > Move Mailbox**.
- Step 4** In the Move Mailbox To list, click the server to which the mailbox(es) will be moved.
- Step 5** Click **OK** to move the mailbox(es).
- Step 6** Once the mailbox(es) have been moved, subscribers may not be able to access messages until the directory is updated. You can either force directory replication, or you can wait for the directory replication to occur automatically, depending on your Exchange settings.
- Before you force directory replication, it is a good idea to discuss this with the Exchange administrator for your site. If you decide to force directory replication, do so for the Cisco Unity server where the mailbox(es) used to reside and for the server to which the mailbox(es) were moved. Refer to the Microsoft Exchange 5.5 documentation for detailed procedures.
- Step 7** Continue with the following procedure.
-

To Synchronize the Servers

Repeat this procedure for each Cisco Unity server from which subscribers have had their mailboxes moved in the previous procedure.

- Step 1** In the Bulk Subscriber Logout window, click the **Resynch Subscribers** button, and follow the on-screen instructions. This step synchronizes the Cisco Unity cache with the Exchange 5.5 directory, logging Cisco Unity back into the subscriber mailboxes.
- Step 2** Click **Exit**.
- Step 3** Notify subscribers that they can log on to both Outlook and Cisco Unity.
-

To Run the Exchange 5.5 Optimizer

If you have moved more than 100 subscribers in Exchange 5.5, run the Exchange Optimizer on the Cisco Unity server. Otherwise, you may encounter problems with Cisco Unity not accepting dialed extensions for subscribers and call handlers, and with conversation-related errors in the event log. If there are other Exchange servers in the site, you do not need to run the Exchange Optimizer on the other Exchange servers.

-
- Step 1** Shut down the Cisco Unity server, if it is running.
- Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > Microsoft Exchange Optimizer**.
- Step 3** Follow the on-screen instructions. If the Exchange Optimizer recommends that you move files, you can safely choose not to do so.
- Step 4** If the Exchange 5.5 Optimizer displays an error message saying that a service could not be shut down, do the following:
- Exit the **Exchange Optimizer**.
 - Right-click the **Cisco Unity** icon in the status area of the taskbar, and click **Exit**.
 - Start the **Exchange Optimizer**, and follow the on-screen instructions.
- Step 5** When the Exchange Optimizer is finished, restart the Cisco Unity server.
-

Moving the Unity Messaging System, UAmis, and UOmni Exchange Mailboxes

The Unity Messaging System, UAmis, and UOmni mailboxes are special Exchange mailboxes with specific functions. From time to time, you may need to move mailboxes to a server that is faster or has more disk space available, or you may want to move mailboxes when you add new servers to your network.

You use the same procedures to move the Unity Messaging System, UAmis, and UOmni mailboxes that you use to move ordinary subscriber mailboxes in Exchange—but with a few extra steps to prevent problems that can occur after these special mailboxes are moved.

To avoid inadvertently moving the Unity Messaging System, UAmis, or UOmni mailboxes when you move a group of subscriber mailboxes, consider changing their Exchange display names so that these mailboxes are clearly identified as requiring “special” treatment.

The following sections describe the mailboxes and how to move them correctly.

Unity Messaging System Mailbox

When an unidentified caller—an outside caller or a caller from inside the organization calling from a phone that is not associated with a subscriber account (such as a conference room)—leaves a message for a subscriber, Cisco Unity gives the message to the subscriber home server (if not the Cisco Unity server) and stores it in the subscriber mailbox. Such messages are identified as coming from the Unity Messaging System mailbox, which is homed on the server that Cisco Unity gives the message to, and has the display name Unity Messaging System.

For more information on the Unity Messaging System mailbox and its associated account, see the [“Default Accounts” section on page 5-1](#).

To Move the Unity Messaging System Mailbox

-
- Step 1** Use the same procedures that you use for moving ordinary subscriber mailboxes in either Exchange 5.5 or Exchange 2000 as indicated in the [“Moving Subscriber Mailboxes” section on page 9-22](#).

Step 2 To prevent messages from unidentified callers from getting stuck in the Unity Messaging Repository (UMR) after the move, do the following steps:

- a. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- b. From the Services window, stop and restart **AvUMRSyncSvr** service.

Once the UMR service has restarted (it may take a few minutes), Cisco Unity exhibits the following behavior:

- Messages from unidentified callers that are addressed to subscribers who do not have full mailboxes are delivered.
- As expected, messages from unidentified callers that are addressed to subscribers who have full mailboxes are not delivered. However, when Cisco Unity attempts to send a nondelivery receipt (NDR), the NDR gets stuck in the Unity Messaging System mailbox, and is never forwarded to the Unidentified Messages distribution list.

Step 3 To release any stuck NDRs from the Unity Messaging System mailbox, stop and restart the Cisco Unity software by using the system tray icon.

UAmis Mailbox

Outgoing AMIS messages are placed in the special Exchange mailbox that has the display name UAmis_<Servername>. For more information on the UAmis mailbox, refer to the “The UAmis Mailbox” section in the “AMIS Networking” chapter of the *Networking in Cisco Unity Guide*, available on Cisco.com, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guide_books_list.html.

To Move the UAmis Mailbox

Step 1 Use the same procedures that you use for moving ordinary subscriber mailboxes in either Exchange 5.5 or Exchange 2000 as indicated in the “[Moving Subscriber Mailboxes](#)” section on page 9-22.

Step 2 To prevent messages from getting stuck in the UAmis mailbox after the move, stop and restart Cisco Unity by using the system tray icon.

UOmni Mailbox

Administrative messages from the Cisco Unity Bridge to create, modify, or delete Bridge subscribers are placed in the special Exchange mailbox that has the display name UOmni_<Servername>.

To Move the UOmni Mailbox

Step 1 Use the same procedures that you use for moving ordinary subscriber mailboxes in Exchange 2000 as indicated in the “[Moving Subscriber Mailboxes](#)” section on page 9-22.

Step 2 On the Windows Start menu, click **Programs > Administrative Tools > Services**.

Step 3 From the Services window, stop and restart **CsBridgeConnector**, which is the Bridge Connector service.

The Bridge Connector monitors the UOmni mailbox. Restarting it immediately after the mailbox move ensures that the Active Directory contacts that are associated with Bridge subscribers are created correctly and messages do not get stuck in the UOmni mailbox. Once you have restarted the Connector, Bridge subscribers can be added, modified, and deleted without any problems.

Cisco Unity Failover Feature

Failover is a feature that provides a simple redundancy, allowing voice messaging functions to continue if the Cisco Unity server fails or when you need to perform maintenance. To set up failover, you install and configure Cisco Unity on two servers, a primary server and a secondary server.

Under normal circumstances, the primary server is active—Cisco Unity answers phone calls and takes messages, sends message notifications, and turns message waiting indicators (MWIs) on and off. The secondary server is inactive—Cisco Unity is running, but it does not perform any voice messaging functions.

If the primary server fails or if the Cisco Unity service on the primary server stops, the secondary Cisco Unity server automatically becomes active and starts performing standard Cisco Unity operations. This shift from primary to secondary Cisco Unity servers is called failover. If you want to stop the primary Cisco Unity server for maintenance, you can also initiate failover manually.

For details, see the *Cisco Unity Failover Configuration and Administration Guide*, which is available on Cisco.com at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guide_books_list.html.

Backing Up and Restoring a Cisco Unity System

The software installed on a Cisco Unity server includes Windows 2000 Server, SQL Server 2000 or MSDE 2000, and, for some configurations, Exchange 2000. There are a number of suitable backup software products that are tailored to back up this software and the accompanying data. In addition, Cisco Unity includes a Disaster Recovery Tool that you can use to back up and restore Cisco Unity data.

For detailed information on backing up and restoring a Cisco Unity system, refer to the *White Paper: Backing Up and Restoring a Cisco Unity System*, available on Cisco.com at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_technical_reference_list.html.

Cisco Unity Data and Message Storage

Information about subscriber accounts and other Cisco Unity data is stored in a SQL Server database on the Cisco Unity server. Additionally, a small subset of the Cisco Unity information is also stored in the directory. Cisco Unity keeps the information in the directory and in the SQL Server database synchronized.

The directory that Cisco Unity uses for data storage depends on what was selected when Cisco Unity was installed. During installation, you specify a partner Exchange server for Cisco Unity to communicate with. The partner server can be either an Exchange 5.5 or Exchange 2000 server. When the partner server is an Exchange 5.5 server, the directory in which Cisco Unity stores data is the Exchange 5.5 directory. When Exchange 2000 is the partner server, Cisco Unity stores data in Active Directory.

By storing its data in a SQL Server database, Cisco Unity derives many performance, reliability, and scalability benefits. Because very little information is stored in the directory, and because that information is not likely to change often, directory replication caused by changes to Cisco Unity data is minimal after the initial creation of subscriber accounts.

Cisco Unity Functions When the Network Is Down

In addition to the SQL database that contains subscriber names and extensions, the Unity Messaging Repository (UMR) is also on the Cisco Unity server. When an Exchange server or even the entire Exchange network is down, Cisco Unity can answer calls, allow unidentified callers to look up subscriber extensions, and take voice messages. While the e-mail system or network is off line, new voice messages are stored in the messaging repository on the Cisco Unity server. During this time, subscribers checking their voice messages hear the UMR conversation, which explains that their Exchange server is not available but lets them access voice messages left from the time that it went down. When the Exchange server or network is back on line, the voice messages stored in the messaging repository are routed to the subscriber mailboxes.