



Configuring Cisco Unity for Maintenance Tasks

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 2-1](#) 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 the authentication method that it uses. To learn more about the authentication methods that you can use with the Cisco Unity Administrator and the Status Monitor, refer to the “About Cisco Unity Administrator Authentication” section in the “Accessing the Cisco Unity Administrator” chapter in the *Cisco Unity System Administration Guide*. For more information on the accounts that you can use to access Cisco Unity, refer to the “About the Accounts That Can Be Used to Administer Cisco Unity” section in the same chapter. The *Cisco Unity System Administration Guide* is available at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag404/ex/index.htm.

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 applicable 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 for an applicable 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 enter the user name, password, and domain for an applicable Windows domain account, and click **Log On**.

Table 2-1 describes each page in the Status Monitor.

Table 2-1 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 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 updating subscriber properties, archiving messages, deleting messages, and running detailed mailbox status reports, all according to configurable schedules.

The Message Store Manager utility allows administrators to set up subscriber groups, called agents. Each action that an administrator sets up the Message Store Manager utility to do 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. 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, you can configure and schedule tasks to be run daily, weekly, or monthly, according to the needs of your site.

For more information on setting up agents and using the Message Store Manager utility, refer to the utility Help.

Subscriber Message Store Status Report

The Subscriber Message Store Status report is one of the maintenance tools available in the Message Store Manager utility. The 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, whether “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_<mmddyy>_<hhmmss>.csv. Report files are saved in the Temp directory of the account that is used to run the report. You may want to move the report files to a different location for storage. Periodically delete report files that you no longer need in order to conserve disk space.

Event Monitoring Service

The Event Monitoring Service (EMS) utility sends e-mail, voice messages, or both to subscribers or public distribution lists in response to an error condition or potential problem on the Cisco Unity server. The EMS can also send SNMP alerts and syslog notifications for Simple Network Management Protocol (SNMP) configurations. The utility monitors the Windows application log and sends a notification when a specified event occurs, such as “Disk almost full.”

The EMS has one predefined event notification, All Unity Errors, that sends notification for all errors that originate from a Cisco Unity component. This predefined event notification is disabled by default and cannot be deleted. However, you can modify the All Unity Errors event by excluding individual sources.

By using the EMS, you can do the following:

- Create new event notifications
- Modify existing event notifications
- Add recipients

- Delete recipients
- Enable and disable event notifications
- Individually enable and disable the receipt of event notifications for specific recipients
- Configure how frequently recipients are notified for a particular event
- Choose the message type with which EMS notifies recipients (for details, see [Table 2-2](#))

Table 2-2 Types of Message Notifications That EMS Can Send

Message Type	Description
Voice message	A recorded notification is sent to one or more subscribers or public distribution lists. With this option, you can use the default message, or you can record the message you want to be sent. The recording must be a WAV file. If Cisco Unity is configured for failover, the WAV file must also be saved on the secondary server. You can use a recording and playback device on the active primary server to record your message. (Refer to the “Using the Media Master to Record Greetings and Names” section in the “Using the Cisco Unity Administrator” chapter of the <i>Cisco Unity System Administration Guide</i> for more information about making recordings.)
E-mail message	A text message is sent to one or more subscribers or public distribution lists.
SMTP message	A text message is sent by using the SMTP server included with IIS. This capability is useful when you want to send notification through the Internet to an e-mail address at another location. Because this method does not depend on Cisco Unity for the notification, it can be used to monitor events that indicate catastrophic failure of Cisco Unity.
SNMP trap	SNMP trap notification works with the Remote Serviceability Kit (RSK) to allow you to configure SNMP notifications for monitored Windows Event log entries. You configure the SNMP destinations via the SNMP Service properties in the Services configuration manager in Windows. For information on setting up SNMP on the Cisco Unity server, see the “ Setting Up SNMP Notification ” section on page 2-5.
Syslog	A Windows Event log entry is sent through the IP network to a syslog server.
Failover	Failover notification initiates a failover on any event for which this recipient is enabled. Use this type of notification with extreme caution. Create a unique recipient for failover notification and use this recipient only for very specific Cisco Unity error events.

The EMS monitors the Windows Event logs; 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, refer to the “Event Log Report” section in the “Reports” chapter of the *Cisco Unity System Administration Guide*. 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 Help.

**Note**

The *Cisco Unity System Administration Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag404/ex/index.htm.

Setting Up SNMP Notification

Do the following procedures if you want to use SNMP notification with the EMS. Refer to the Microsoft Windows Help for additional SNMP configuration information.

To Set Up the Remote Serviceability Kit

- Step 1** On the Cisco Unity server, double-click the **Cisco Unity Tools Depot** icon.
 - Step 2** In the left pane, under Diagnostic Tools, double-click the **Remote Serviceability Kit Configuration Wizard**.
 - Step 3** Follow the on-screen instructions.
 - Step 4** Continue with the following [“To Set Up SNMP Security”](#) procedure.
-

To Set Up SNMP Security

The Windows 2000 SNMP agent provides security through the use of community names and authentication traps.

-
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Settings > Control Panel > Administrative Tools > Services**.
 - Step 2** Right-click the **SNMP Service**.
 - Step 3** Click **Properties**.
 - Step 4** Click the **Security** tab.
 - Step 5** In the Accepted Community Names field, click **Add**.
 - Step 6** In the Community Name field, enter the name of the community.
 - Step 7** In the Community Rights field, choose either **Read-Only** or **Read-Write**. (If you want to be able to change the Cisco Unity configuration parameters, choose **Read-Write**.)
 - Step 8** Click **Add**.
 - Step 9** Choose the **Accept SNMP Packets from These Hosts** option if you want to allow only specific Network Management System (NMS) hosts to query the SNMP extension agent.
 - Step 10** Click **Add**.
 - Step 11** Enter the IP address for the hosts that are allowed to query the SNMP extension agent.
 - Step 12** Click **Add**.
 - Step 13** Check the **Send Authentication Trap** check box if you want to receive SNMP authentication failure traps.
 - Step 14** Continue with the following [“To Set Up the SNMP Trap Receiver”](#) procedure. Do not exit from the SNMP Properties page.
-

To Set Up the SNMP Trap Receiver

- Step 1** Click the **Traps** tab.

- Step 2** In the Community name field, enter the community name to be used in the trap messages that are generated from this host.
- Step 3** Click **Add to List**.
- Step 4** In the Trap Destinations field, click **Add**.
- Step 5** In the Trap Destinations field, enter the IP address or hostname of the trap destination.
- Step 6** Click **Add**.
- Step 7** Repeat [Step 4](#) through [Step 6](#) for each trap destination that is required.
- Step 8** Click **OK**.
- Step 9** Continue with the following “[To Start the Cisco Unity SNMP Extension Agent](#)” procedure. Do not exit from the SNMP Properties page.

To Start the Cisco Unity SNMP Extension Agent

The SNMP service should start automatically when the Cisco Unity server is started or restarted. Do this procedure to confirm that the service is configured properly and to start it if it is not currently running.

- Step 1** Click the **General** tab.
 - Step 2** Confirm that the Startup Type is **Automatic**. If the Startup Type is set to any other value, change it to **Automatic**.
 - Step 3** Confirm that the Service Status is **Started**. If the status is set to any other value, click **Start**.
 - Step 4** Click **OK**.
-

Setting Up Event Notification

Do the following procedure to set up event notification. For instructions on modifying events, message types, or recipients, refer to the EMS Help.

To Set Up Event Notification

- Step 1** On the Cisco Unity server, click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane of the Tools Depot window, expand **Diagnostic Tools**, and double-click **Event Monitoring Service**.
- Step 3** If you are starting the Event Monitoring Service for the first time, when prompted, enter the password for the account that the AvCsMgr service logs on as, and click **OK**. Otherwise, continue with [Step 4](#).
- Step 4** On the File menu, click **New > Recipient**. The Create New Recipient dialog box appears.
- Step 5** In the Recipient Name field, enter a name for the recipient.
- Step 6** To select the methods of notification for this recipient, complete the information on one or more of the tabs as applicable:
 - Click the **Voice Mail** tab. Select either a **Subscriber** or a **Distribution List**.
 - Click the **E-Mail** tab. Select either a **Subscriber** or a **Distribution List**.

- Click the **SMTP** tab. Enter a fully qualified SMTP address that you want to receive notification. Click >> to add one or more SMTP addresses to the SMTP Addresses list.
- Click the **SNMP Trap** tab. Check the **SNMP Trap Enabled** check box.
- Click the **Syslog** tab. Check the **Enabled** check box. In the Server field, enter the IP address of the syslog server that you want to receive the Event log message.
- Click the **Failover** tab. We recommend that you create a unique recipient that is used only for initiation of failover.

Step 7 Click **OK**.

Step 8 In the File menu, click **New > Event**. The Add New Event dialog box appears.

Step 9 In the Source list, click the name of the source for the error you want to monitor. Or, you can import an event that you have copied from the Windows Event log to the clipboard.

Step 10 Under ID, click one of the following:

All Event IDs	Sends notification for all Event log messages from the source you selected in Step 9 .
Specific Event ID	Sends notification only for the Event ID you enter in the field to the right of this option.

Step 11 In the Type list, click one of the following:

Errors	Sends notification only for error events that appear in the Event log.
Errors & Warnings	Sends notification for error and warning events that appear in the Event log.
Errors, Warnings & Informational	Sends notification for error, warning, and informational events that appear in the Event log.

Step 12 Check the **Active** check box.

Step 13 In the Notes field, enter text to indicate what this event monitors.

Step 14 To configure a voice message for use with message notifications, continue with [Step 15](#).

To configure e-mail or SMTP content for use with message notifications, continue with [Step 16](#).

Step 15 Select a voice message for use with voice message notifications by doing the following sub-steps:

- To the right of the Voice Mail File Name field, click **...**, browse to the WAV file you want to use as the voice message, and click **OK**. EMS will send this recording as a voice message.
- In the Voice Mail Priority list, click **Urgent**, **Normal**, or **Low**, as applicable.
- Continue with [Step 17](#).

Step 16 Configure e-mail or SMTP content for use with e-mail or SMTP notifications by doing the following sub-steps:

- In the E-Mail Subject field, enter the subject line for the e-mail or SMTP notification that EMS will send. You can enter text, or right-click to see a menu of insertion strings that EMS provides. For example, you can enter **Cisco Unity Failover Occurred**.
- In the E-Mail Priority field, click **Urgent**, **Normal**, or **Low**, as applicable.

- c. In the E-Mail Body field, accept the default body text, or enter customized text for the e-mail or SMTP notification that EMS will send. You can enter text, or right-click to see a menu of insertion strings that EMS provides.
 - d. Click **OK**.
 - e. Continue with [Step 17](#).
- Step 17** In the right pane of the Event Monitoring Service window, under Recipients, click the **Add Recipients** icon.
- Step 18** In the Edit Recipients for Event dialog box, check the **Active** check box for the recipients you want to receive the event notification, and click **OK**.
- Step 19** Near the top of the right pane, click **Apply**.
- Step 20** Close the Event Monitoring Service window and the Tools Depot window.
-

Best Practices for Managing Subscriber Mailbox Size

You can manage subscriber mailbox size in the following ways:

Understand How Cisco Unity Handles Full Mailboxes and How Performance Is Affected by Mailbox Size

To learn more about how Cisco Unity handles subscribers with full mailboxes, refer to the “How Cisco Unity Handles Full Mailboxes” section in the “Default Accounts and Message Handling” chapter of the *Cisco Unity System Administration Guide*. (The *Cisco Unity System Administration Guide* is available at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag404/ex/index.htm.)

Because the processing of messages happens in real-time when the users log on to check their messages, mailbox size directly affects Cisco Unity conversation performance. For mailbox size recommendations and other performance considerations, see the “Administrative Monitoring Guidelines for Cisco Unity Performance” section on page 7-8.

Set Appropriate Size Limits on Subscriber Mailboxes

Setting lower size limits on subscriber mailboxes can help prevent the hard disk of the server where messages are stored from running out of space. You can use the Message Store Manager utility (see the “Message Store Manager Utility” section on page 2-3) to view and set mailbox size limits, or you can use the procedures in the “Setting a Maximum Size for Exchange Mailboxes” section on page 3-1 to do so in Exchange.

For more information on Exchange 5.5, Exchange 2000, and Exchange 2003 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/univercd/cc/td/doc/product/voice/c_unity/whitpaper/e2kstore.htm.

Enforce a Message Retention Policy

You can manage the size of subscriber mailboxes by automatically deleting messages from mailboxes based on the criteria outlined in the message retention policy for your organization. For example, a message retention policy may specify that messages are permanently deleted from the message store server after 30 days, three months, or another period of time. (Check with members of the Legal and Information Systems groups in your organization for advice on defining a message retention policy for the organization.)

Periodically deleting messages from subscriber mailboxes can prevent the hard disk on the server where messages are stored from filling up, and may be an especially important practice if the subscribers in your organization have class of service rights to save and manage their deleted messages, but do not often remember to permanently delete them.

You can use the Message Store Manager utility (see the “[Message Store Manager Utility](#)” section on [page 2-3](#)), to automatically purge subscriber messages according to the schedule you specify. To set up this functionality, refer to the Message Store Manager utility Help. When you are ready to enforce the message retention policy for your organization, notify subscribers. If subscribers know that their saved, sent, and deleted messages (as applicable) are only stored on the server for a certain period of time, they can plan to archive or move messages themselves and you can reduce support desk requests for “lost” messages.

Prevent Mailboxes From Filling Up While Subscribers Are on Vacation or on an Extended Leave of Absence

For as long as a subscriber alternate greeting is enabled, you can specify that Cisco Unity prevent all callers from leaving messages for the subscriber, which can help reduce mailbox size when subscribers are out of the office and do not plan to check messages regularly. In addition, you can increase caller awareness of a subscriber absence by specifying that Cisco Unity prevent all callers from skipping the greeting.

To set caller options for a subscriber alternate greeting, refer to the “Subscriber Greetings Settings” section in the “Subscriber Settings” chapter in the *Cisco Unity System Administration Guide*. (The *Cisco Unity System Administration Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag404/ex/index.htm.)

Train Subscribers to Better Manage Their Own Mailbox Size

Subscribers can make room in their mailboxes by deleting messages (including messages in the Sent and Deleted Items folders in Microsoft Outlook or the Cisco Unity Assistant, if applicable). To archive a message before deleting it, subscribers can use the Copy to File option available from the Options menu on the Media Master control bar, and save the file to their hard drives. Unified Messaging subscribers can use Outlook to move messages to private folders that they set up on their hard drives.

For these and more tips, refer subscribers to the “Managing Your Mailbox Size” section in the “The Tools You Use” chapter of the *Cisco Unity User Guide*. (The *Cisco Unity User Guide* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/ug/ug404/ex/index.htm.)

