



Reports

Overview: Reports

You can use Cisco Unity reports to gain information about subscribers and system activity. Some Cisco Unity reports provide information about subscribers and system activity over a period of time. Others offer a “snapshot” of a particular Cisco Unity entity as it stands at the time you run the report.

Refer to the following sections in this chapter to learn more about using Cisco Unity reports:

- [About Report Data, page 22-3](#)—This section provides information about how Cisco Unity gathers and stores report data, and which settings you can change to ensure that your reports contain the data you need.
- [Generating Reports, page 22-3](#)—This section details how to generate, view, and print Cisco Unity reports.

Refer to the following sections in this chapter for information on specific reports:

Subscriber reports:

- [Subscribers Report, page 22-5](#)—This report includes profile and account information about each subscriber.
- [Subscriber Message Activity Report, page 22-6](#)—This report shows when subscriber messages were left and when they were accessed.
- [Distribution Lists Report, page 22-8](#)—This report shows the owner, members, and creation date of public distribution lists.

- [Failed Login Report, page 22-8](#)—This report shows details of failed attempts to log on to subscriber accounts (by phone) and to the Cisco Unity Administrator.
- [Storage Usage Report, page 22-10](#)—This report shows the storage limits and disk space used for messages by a subscriber or by all subscribers.
- [Transfer Call Billing Report, page 22-11](#)—This report provides information about call transfers from call handlers and subscribers; this information can be used for billing purposes.
- [Outcall Billing Report, page 22-12](#)—This report provides information about outgoing calls made by Cisco Unity for message notifications; this information can be used for billing purposes.

System reports:

- [Administrative Access Activity Report, page 22-13](#)—This report shows details of all changes entered into the Cisco Unity Administrator; this information can be used as an audit trail of commands entered by system administrators.
- [Event Log Report, page 22-14](#)—This report provides information from the Windows application log.
- [Port Usage Report, page 22-15](#)—This report shows activity on each port; this information can be used to determine when to add new ports.
- [System Configuration Report, page 22-16](#)—This report provides information on system resource allocation.
- [Unresolved References Report, page 22-18](#)—This report shows any call handlers that were left in an invalid state when the Cisco Unity Administrator was not used to delete subscriber accounts.
- [Call Handler Traffic Report, page 22-18](#)—This report shows how many calls are routed through a particular call handler and how callers are choosing to exit that handler.
- [AMIS Out Traffic Report, page 22-20](#)—This report provides information about outbound AMIS calls.
- [AMIS In Traffic Report, page 22-21](#)—This report provides information about inbound AMIS calls.

About Report Data

Cisco Unity reports that provide information about subscribers and system activity over a period of time contain log-based data. For example, the Call Handler Traffic report shows how many calls are routed through a particular call handler and how callers are choosing to exit that handler during the time period that you specify. Other Cisco Unity reports offer a “snapshot” of subscriber or system data as it stands at the time you run the report, and therefore they reflect the current status of a particular Cisco Unity entity. For example, the Storage Usage report shows the current storage limits and disk space used for messages by a subscriber or by all subscribers.

Cisco Unity automatically gathers and stores data that is used in log-based reports every 30 minutes. You specify how long Cisco Unity stores the data in the Cleanup Interval for Logger Data Files in Days field on the System > Configuration > Settings page. For example, if you have set this field to three, a log-based report will reflect activity only for the last three days, even if you specified more than three days in the time range for the report.

You should regularly delete the report files that you generate, to avoid accumulating large amounts of data. By default, Cisco Unity deletes report files every seven days. To change how often reports are deleted, adjust the settings for the Cleanup Interval for Report Files in Days field on the System > Configuration > Settings Page.

Generating Reports

When you generate a report, you can specify some or all of the following:

- The subscribers, administrators, or distribution lists to include in the report
- The date and time range to include
- The sort order for the data in the report

You also choose to save the report either as a Web page or as a comma-delimited file:

Web page	An HTML file. You use a Web browser to view and to print the report. In some cases, a report may be too large to be viewed in a Web browser.
Comma-delimited file	A text file (also known as a comma separated or CSV file). Each row in the report appears on a separate line, and values are separated by commas. Select this format if you want to view the information in another application, for example, a spreadsheet program.

The best time to generate reports is when the system is not busy: after regular business hours when Cisco Unity is not processing many calls, or when there are no other processes running (for example, before or after a full backup). Note that for large systems, reports that offer a “snapshot” of subscriber or system data may take a significant amount of time to run.

In the current release of Cisco Unity, reports cannot be scheduled in advance, and if you turn off Cisco Unity while there are reports in the report queue, the reports will be deleted.

Viewing and Printing Reports

When a report is ready, Cisco Unity sends an e-mail to the person who generated the report. The e-mail contains a link to the report file. To access the report file, all Cisco Unity administrators must have full read/write access and all Domain Users must have read rights to the CommServer\Reports directory located on the Cisco Unity server (these access levels are set by default). To have read rights, an administrator or user must either be a member of the domain that Cisco Unity is in or be associated with a domain that is trusted by the domain that Cisco Unity is in.

All reports contain a report header followed by columns of data. If, for example, you generate a report for all subscribers, the subscriber name is included above the data associated with the subscriber.

To view a report

-
- Step 1** Click the link in the e-mail message.
- Step 2** If the report is in Web page format, the browser will start automatically and display the information. If the report is in comma-delimited format, you may be required to choose an application in which to display the information.
-

To print a report

-
- Step 1** View the report, as described above.
- Step 2** Click **Print** in the File menu.
-

To view the status of a report

The ability to view report status is controlled by class of service.

- Step 1** Go to **http://<server name>/status**, or double-click the desktop shortcut to the Status Monitor.
- Step 2** Click **Reports**.
-

Subscribers Report

Use the Subscribers report to get a listing of all the Cisco Unity subscribers. You can generate the report for an individual subscriber, for all members of a public distribution list, or for all Cisco Unity subscribers.

The Subscribers report includes the following information:

First Name, Last Name	The name of the subscriber or public distribution list for which the report was generated.
Exchange Alias	The subscriber alias in Exchange.
Location	The Cisco Unity location.
NT Domain	The Windows domain name assigned to a subscriber.
Billing ID	The billing ID of a subscriber.
Class of Service (COS)	The class of service assigned to a subscriber.
Extension	The primary phone extension assigned to a subscriber. If there are any alternate extensions assigned to a subscriber, they are listed below the primary.
Inbox Size	The total size, in kilobytes, of all e-mail, voice, and fax messages stored for the subscriber in Exchange.

Subscriber Message Activity Report

Use the Subscriber Message Activity report to diagnose voice message problems reported by a subscriber (for example, voice messages are not being sent or received, or the message waiting indicator is not being turned on or off properly). You generate this report for an individual subscriber only.

The Subscriber Message Activity report includes the following information:

Date and Time	The date and time that the subscriber took action on the message.
Source	Either the computer or the phone that generated the message activity.

Action Taken in Response to Message	<p>The activity that took place in regards to voice messages (for example, New Message, Message Read, Save, Delete, Mark New, Login, and Logoff).</p> <p>The actions MWI On Requested and MWI On Completed indicate, respectively, that Cisco Unity sent a request to the phone system to turn on the MWI and received a request-completed confirmation. In cases where the phone system does not provide a confirmation, Cisco Unity assumes the request was successful.</p>
Number of New Messages	The number of new voice messages in the Exchange mailbox for a subscriber.
Sender's Name and DTMF	The name and extension of the message sender, if known.
Date and Time Message Arrived	The date and time the message arrived in the Exchange mailbox.
Dial Out Number	The number to which a message notification was sent.
Dial Out Result	<p>The result of the outgoing call for the message notification. Possible results include:</p> <ul style="list-style-type: none">• Busy—The dialed number was busy.• Connected—The called party answered the phone.• Failure—The call failed.• Port Disabled—All ports for outgoing calls were disabled.• Port Unavailable—No ports were available for the outgoing call.• RNA (Ring No Answer)—The dialed number did not answer.• Release—The result is unknown. This typically happens for notifications sent to pagers.• Unknown—The result is unknown.

Distribution Lists Report

Use the Distribution Lists report to get a listing of all public distribution lists and, optionally, the members in each list. You can generate the report for a selected public distribution list or for all public distribution lists.

If you want the report to include the names of distribution list members, check the List All Members For Each Distribution List check box.

The Distribution Lists report includes the following information:

Creation Date	The date that the public distribution list was created.
List Alias	The Exchange alias name of the public distribution list.
Count	The number of subscribers and other public distribution lists that are members of the public distribution list.
Distribution List Name	The name of the public distribution list.
Owner First and Last Name	The subscriber or public distribution list that owns the public distribution list.
Member List	The names of subscribers and other public distribution lists that are members of this public distribution list.

Failed Login Report

The Failed Login report includes information about failed phone user logons as well as failed Cisco Unity Administrator logons. Use the Failed Login report to identify patterns of invalid logons, which would indicate that an individual is trying to gain unauthorized access to Cisco Unity. The report also identifies accounts that have been locked because the maximum number of invalid logons has been exceeded.

You can generate the Failed Login report for an individual subscriber account, or for all subscriber accounts. Additionally, you can indicate whether to show all failed logon attempts (expand the report) or show only the last failure for each subscriber.

Note that including the Failed Login report for the Cisco Unity Administrator logons requires that auditing be enabled in system security policies. Cisco Unity setup enables auditing by default.

The Failed Login report includes the following information about failed phone user logons:

Subscriber/User Name	The display name of the subscriber whose account experienced the failed logon.
Alias	The Exchange alias of the subscriber whose account experienced the failed logon.
Caller ID (Phone Number Called From)	The calling number, if known, from which the logon was attempted.
Subscriber DTMF	The unique DTMF access code that callers dial to access this account.
Date and Time	The date and time of the failed logon.
Maximum Failures Exceeded	Whether the failed logon exceeded the maximum number allowed; if so, the account is locked.
Failure Number	A running total of failed logons by subscriber or by day, depending on how the report is sorted.
Source	Indicates either Standard when a subscriber uses normal Cisco Unity password security, or Enhanced when a subscriber uses enhanced phone security to log on.

The Failed Login report also includes the following information about failed Cisco Unity Administrator logons:

User Name	The logon name assigned to the subscriber.
Computer	The name of the workstation, if known, from which a subscriber attempted to log on.
User Domain	The Windows domain name assigned to a subscriber.
Event ID	The Windows event ID that was generated when the logon failed.
Date and Time	The date and time of the failed logon.
Failure Number	A running total of failed logons by subscriber or by day, depending on how the report is sorted.

Storage Usage Report

Use the Storage Usage report to obtain information about the amount of storage space available and the disk space used for storing messages by each subscriber. You can generate the Storage Usage report for a selected subscriber, for all subscribers, or for a public distribution list.

The Storage Usage report includes the following information:

Subscriber Name	The display name of the subscriber.
Storage Limit (KB)	The amount of disk space, in kilobytes, allocated for the subscriber message store.
Total Message Size (KB)	The amount of disk space, in kilobytes, in use for received and stored messages.
Disk Storage Available (KB)	The amount of disk space, in kilobytes, available for receiving and storing messages.

Transfer Call Billing Report

Use the Transfer Call Billing report to obtain information about calls that are transferred from a subscriber account or from a call handler. You can use this report for billing purposes or to keep track of transfers to long distance phone numbers. You can generate the report for all subscribers, billing IDs, or call handlers, or for a specific subscriber, public distribution list, billing ID, or call handler.

The Transfer Call Billing report includes the following information:

Name	The name of the Cisco Unity entity (such as subscriber, call handler, or interview handler) from which the call was transferred.
Extension	The extension of the Cisco Unity entity (such as subscriber, call handler, or interview handler) from which the call was transferred.
Billing ID	The billing ID of the Cisco Unity entity (such as subscriber, call handler, or interview handler) from which the call was transferred.
Date	The date that the transfer occurred.
Time	The time that the transfer occurred.
Dialed Number	The number that the call was transferred to.
Transfer Result	The result of the call. Possible results include: <ul style="list-style-type: none">• Connected—The called party answered the phone.• Busy—The dialed number was busy.• RNA (Ring No Answer)—The dialed number did not answer.• Released—The result is unknown.

Outcall Billing Report

Use the Outcall Billing report to obtain information about outbound calls made by Cisco Unity for message notifications. This report also provides information about outbound calls made when subscribers use the Media Master control bar to create or play recordings over the phone. You can use this report for billing purposes, or to keep track of message notifications sent to long distance phone numbers.

You can generate the report for all Cisco Unity subscribers or billing IDs, or for a specific subscriber, billing ID, or public distribution list. You can select to generate a summary version of the report or a detailed version, which includes the times and lengths of each call.

The detailed version of the Outcall Billing report includes the following information:

Name	The name of the Cisco Unity entity (such as subscriber, call handler, or interview handler) which made the call.
Extension	The extension of the Cisco Unity entity (such as subscriber, call handler, or interview handler) which made the call.
Billing ID	The billing ID of the Cisco Unity entity (such as subscriber, call handler, or interview handler) which made the call.
Time	The time that Cisco Unity made the call.
Delivery Device	The notification device that the message was sent to, which can be a home phone, work phone, spare phone, or pager. For Media Master recording by phone, the word “TRAP” (Telephone Record And Playback) is listed as the delivery device.
Dialed Number	The phone number of the delivery device.

Result	The result of the call. Possible results include: <ul style="list-style-type: none">• Busy—The dialed number was busy.• Connected—The called party answered the phone.• Failure—The call failed.• Port Disabled—All ports for outgoing calls have been disabled.• Port Unavailable—No ports were available for the outgoing call.• RNA (Ring No Answer)—The dialed number did not answer.• Release—The result is unknown. This typically happens for notifications sent to pagers.• Unknown—The result is unknown.
Call Time (Seconds)	The length of the call, in seconds.

Administrative Access Activity Report

Use the Administrative Access Activity report to track which system administrators changed values in Cisco Unity during a specified period and the changes they made. You can generate this report for a selected administrator or for all administrators.

The Administrative Access Activity report includes the following information:

Date and Time	The date and time that the administrator created, deleted, or updated data for a Cisco Unity entity (such as subscriber, call handler, or interview handler).
Admin	The administrator alias in Exchange.
Administrator's First and Last Name	The name of the administrator.

DTMF ID	The extension assigned to the administrator.
Administrative Action	Whether the administrator action created, updated, or deleted data for a Cisco Unity entity.
Object	The type of Cisco Unity entity (such as subscriber, call handler, or interview handler) that the administrator created, deleted, or updated.
Name	The name of the Cisco Unity entity (such as subscriber, call handler, or interview handler) that the administrator created, deleted, or updated.
Field (Property)	The name of the field from the page in the Cisco Unity Administrator that was changed in creating, updating, or deleting data for a Cisco Unity entity.
Value	The new value for the changed field.

Event Log Report

Use the Event Log report to list events from the Windows application log. You can generate the report for all application events on the Cisco Unity server, or for the events that apply only to Cisco Unity. Note that Cisco Unity writes events only to the Windows application log; it does not write events to the system or security logs. If you generate a report for all application events, you can identify the Cisco Unity events as those events that end in “_MC” (for example, “AvLogMgrSvr_MC”).

You can also view application events by using the Windows Event Viewer (from the Start menu, click Programs > Administrative Tools > Event Viewer). For more information on Windows events, refer to the Windows Event Viewer online Help. If you want Cisco Unity to send e-mail, voice mail, or both to subscribers or public distribution lists in response to an application event on the Cisco Unity server, see the [“Event Notification Utility” section on page 6-3](#) to set this up.

The Event Log report includes the following information:

Date and Time	The date and time that the event occurred.
Type	The Windows event type.
Source	The component that caused and logged the event.
Message (Msg) ID	The event ID.
Computer	The server on which the event occurred.
More Info	A message that contains additional information about the event.

Port Usage Report

Use the Port Usage report to determine if the voice messaging system is running close to capacity. You can indicate the port or ports to include in the report. Enter port numbers or ranges of numbers separated by commas (for example, 1,2,4,8) in the Ports to Show field. To include all ports in the report, leave this field blank.

The Port Usage report includes the following information:

Port Number	The Cisco Unity port number.
Unit of Time	The unit of time by which data is broken down for the time period that you specified in the Date Range. Depending on the length of the time period, data is broken down into hours, days, and weeks.
Date Range	The range of dates for which data is included.
Time	The specific hour or date(s) by which data is broken down for the time period that you specified in the Date Range.
Ports	The ports included in the report.

Number of Calls	The number of calls processed by the port per hour, day, or week for the time period specified.
Length of Calls	The total length, in seconds, of all calls on the port per hour, day, or week for the time period specified.
Average Length of Calls	The average length, in seconds, of all calls on the port per hour, day, or week for the time period specified.
Percent Utilization	<p>The percentage of available time that a port was in use per hour, day, or week.</p> <p>Note that it is recommended that the value of Percent Utilization not exceed 80 percent of the ports used for incoming calls during peak usage.</p>
Average Calls Per Hour	The average number of calls per hour for each port.
Average Calls Per Day	The average number of calls per day for each port. This information is provided only on the row that contains the summary for the week.

System Configuration Report

Use the System Configuration report to get information about the Cisco Unity server and software.

You also can view this information in the Cisco Unity Administrator on the Configuration pages.

The System Configuration report includes the following information:

Serial Number	The serial number that appears on the system key.
OEM Code	Identifies the OEM version, if applicable.
Product	The name of the software product and version number.

Number of Voice Ports	The number of voice ports licensed for the Cisco Unity system.
Languages	The number of language licenses.
Available Licenses and Total Licenses	The available and total number of Cisco Unity licensed features, such as text-to-speech and Digital Networking.
Leading Silence for Recordings	The length of silence, in seconds, allowed at the beginning of a recording. When the leading silence is longer than specified, Cisco Unity stops recording and discards the recording.
Trailing Silence for Short and Long Recordings	The length of silence, in seconds, allowed at the end of recordings that are 30 seconds or less and of recordings that are more than 30 seconds. When the trailing-silence limit is reached, Cisco Unity assumes the recording is finished and stops recording.
Minimum Length for a Recording	The minimum length of a recording, in seconds. When a recording is shorter than the minimum length, it is discarded.
Computer and Domain Name	The Cisco Unity server name on the network and the Windows domain name.
Total Hard Drive Space, Total Used Hard Drive Space, and Total Free Space	The total size of all hard disks, the total amount of space in use, and the total free space on the Cisco Unity server.
Additional Settings	The report contains additional information about the Cisco Unity server and software, such as integration type, ActiveAssistant licensing, and the text-to-speech engine.

Unresolved References Report

Use the Unresolved References report to locate primary call handlers (those call handlers that are associated with a subscriber account), other call handlers, and interview handlers that are left unresolved because of the improper deletion of a subscriber account. The problem occurs when a subscriber is deleted by using Microsoft Exchange or Windows administrator applications without first deleting the subscriber by using the Cisco Unity Administrator.

The Unresolved References report examines the Cisco Unity information stored in the Exchange directory and reports any problems that it finds. The report identifies the unresolved handler, describes the problem, and suggests a solution.

If the report finds an unresolved primary call handler, you will need to use the Cisco Unity SysCheck utility to remove it. To access the SysCheck utility, go to the directory in which Cisco Unity is installed (the default is C:\CommServer). Then, browse to the SysCheck subdirectory, and run SysCheck.exe.

The Unresolved References report includes the following information:

Handler Name	The name of the unresolved handler.
Handler/Access ID	The extension (if any) associated with the handler.
Handler Type	The type of handler found to be in an unresolved state. The type can include call handlers, interview handlers, the directory handler, or primary call handlers.
Owner	The owner of the handler.
Message Recipient	The message recipient associated with the handler.

Call Handler Traffic Report

Use the Call Handler Traffic report to track the number of calls routed by a particular call handler, and how callers chose to exit that handler.

There are four ways a caller can exit a call handler: by hanging up, by choosing a one-key dialing option, by dialing an extension that transfers the call to another call handler (or subscriber), or by being routed automatically by the after-greeting action specified in the call handler.

The Call Handler Traffic report includes the following information:

Start Time	The specific hour or date(s) by which data is broken down for the time period that you specified in the Date Range.
Total Calls	The total number of calls routed to the call handler.
Method Callers Use to Exit a Call Handler	The total number of times each exit method is used by callers. Callers can exit a call handler by hanging up, pressing a one-key dialing option, dialing an extension that transfers the call to another call handler (or subscriber), or by being routed to another call handler (such as the Good-Bye call handler) as specified by the after-greeting action.
Key	The number of calls in which the caller exited the call handler by pressing a one-key dialing option. The report includes a tally for each key.
DTMF ID	The number of calls in which the caller exited the call handler by dialing a valid extension to transfer to another call handler (or subscriber).
Invalid DTMF ID	The number of calls routed to the default Error call handler because the caller dialed an invalid extension.
After Greeting Action	The number of calls routed according to the after greeting action specified for the call handler.
Hang-Up	The number of calls in which the caller exited the call handler by hanging up.

AMIS Out Traffic Report

Use the AMIS Out Traffic report to track the progress of outbound AMIS messages. This report is available only if your organization purchased a license for AMIS.

The Outbound AMIS Traffic report includes the following information:

Submit Date and Time	The date and time that the AMIS message transmission was completed.
Importance (Urgency)	Indicates whether the subscriber marked the AMIS message “Urgent” before sending it to the destination node.
Sender’s Primary Extension/Sender	The extension of the subscriber who sent the AMIS message to the destination node.
Target Device/Target Mailbox Delivery Number	The remote mailbox ID number of the AMIS message recipient.
Transmission Start Time	The date and time that Cisco Unity started the transmission of the AMIS message to the destination node.
Transmission Duration	The total number of seconds needed to transmit the AMIS message from one node to the other.
Delivery Status	“Sent OK” is specified for successful deliveries and “Failed” for failed deliveries; if available, a brief explanation is displayed.
Total Transmission Time	The total transmission time for all AMIS messages sent, specified in seconds.

Total Messages Delivered Successfully	The total number of AMIS messages that were delivered within their specified delivery schedules.
Total Failed Messages	The total number of AMIS messages that were not delivered to the destination node within their specified delivery schedules.

AMIS In Traffic Report

Use the AMIS In Traffic report to track the progress of inbound AMIS messages. This report is available only if your organization purchased a license for AMIS.

The AMIS In Traffic report includes the following information:

Start Reception/Transmission Receive Time	The date and time that Cisco Unity began receiving the transmission of the AMIS message.
Matching ID/Remote Sender ID	The remote mailbox ID number of the remote subscriber sending the AMIS message. If Cisco Unity cannot find a matching ID for the node that sent a message, this section in the report is left blank, and the delivery is reported as a failure in the Status column.
Target User's Primary Extension/Recipient Extension	The extension of the subscriber for whom the AMIS message is intended. If Cisco Unity cannot find the subscriber extension in the directory, this section in the report is left blank, and the delivery is reported as a failure in the Status column.
Transmission Duration	The total number of seconds needed to transmit the AMIS message from one node to another.
Delivery Status	“Received OK” is specified for successful deliveries and “Failed” is specified for failed deliveries; if available, a brief explanation is displayed.

Port Number	The number of the port that received the AMIS message.
Total Transmission Time	The total transmission time for all AMIS messages that were received, specified in seconds.
Total Messages Received Successfully	The total number of AMIS messages that were received within their specified delivery schedules.
Total Failed Messages	The total number of AMIS messages that were not received within their specified delivery schedules.