555-7101-310

CallPilot

Reporter Guide

Product release 2.02 Standard 1.0 May 2003

NORTEL NETWORKS™

CallPilot

Reporter Guide

Publication number:	555-7101-310
Product release:	2.02
Document release:	Standard 1.0
Date:	May 2003

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

The process of transmitting data and call messaging between the Meridian 1 and CallPilot is proprietary to Nortel Networks. Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

This page and the following page are considered the title page, and contain Nortel Networks and third-party trademarks.

Publication history

May 2003
Released as Standard 1.0 for CallPilot 2.02.

March 2002
Preliminary 0.03 of the *CallPilot Reporter Guide 2.0* is issued for Beta trial review. This issue has been updated with Alpha Trial review comments.

September 2002
Released *CallPilot Reporter Guide 2.0* as Standard issue.

December 2001
Draft 0.02 of the *CallPilot Reporter Guide 2.0* is issued for Alpha Trial review. This issue uses A5-size templates, contains updated information, and has been edited for style.

January 2001
Draft 0.01 of the *CallPilot Reporter Guide 2.0* is started.

Contents

Creating reports and alerts 35

Viewing reports and alerts 43

Customizing reports and alerts 47

Chapter 1

Getting started with Reporter

In this chapter

Overview of CallPilot Reporter

Introduction

Reporter is a web-based application that helps you analyze and manage your CallPilot system. Reporter converts raw statistics from your server into easy-to-read reports.

- **View on demand**—View reports and alerts at any time for a period that you specify.
- **Customize**—Customize reports to include relevant data only. For example, you can filter the data in a report to show activities that occur in a particular department. For more information, see Section D: “Customizing reports and alerts,” on page 47.
- **Print**—Schedule reports to print on a regular basis, or print reports on demand. When you use a print schedule, you can monitor system usage over a period of time and identify patterns and trends. You can also set up alerts to print when they are triggered. For more information, see Section E: “Printing and exporting reports and alerts,” on page 57.
- **Export**—Export report information to a variety of file formats so that you can easily distribute the information to others who need it. For example, you can display exported reports on the World Wide Web, over an organizational intranet, or in a spreadsheet program. For more information, see Section E: “Printing and exporting reports and alerts,” on page 57.

About this guide

The *Reporter Guide* provides information required to

- generate reports and alerts
- analyze and interpret report and alert data

Feature availability

To use Reporter, you must have Full Administrator rights or Reporter Administration rights enabled in CallPilot Manager.

What’s new in this guide

- **New web-based interface**—Reporter is easier to use, and report generation is faster.
- **Increased accessibility**—You no longer need to schedule and download data to your computer to generate reports. Data remains on your web server and is available at all times.
- **Personalized settings**—Reporter can save your custom reports, settings, and log for future sessions. This saved information is called a profile. For more information about profiles, see “Reporter profiles” on page 74.
- **Event logging**—The Reporter Log tracks changes that you perform. The log is a part of your Reporter profile.
- **New reports**—Reporter includes an Administration Action report to track changes made by administrators.

Overview of reports and alerts

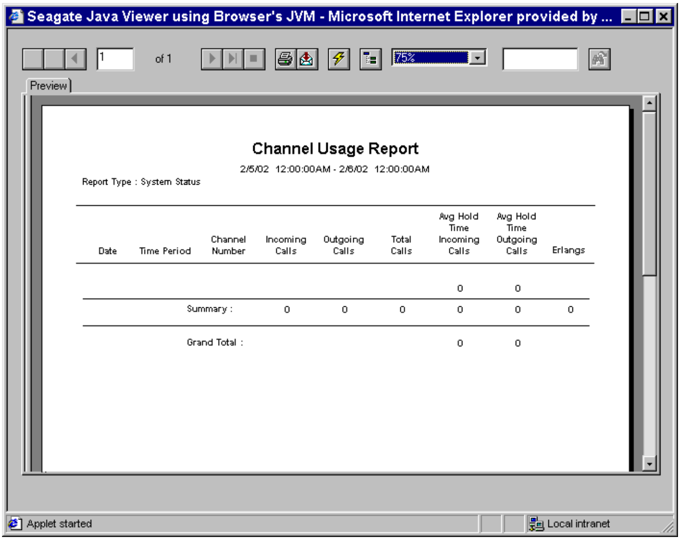
Introduction

Reports organize the operational measurements (OMs) collected by your server into a format that you can study and analyze. When you study reports over a period of time, you can identify trends and patterns related to system usage. With this information, you can improve the overall efficiency of your system, increase system security, and troubleshoot potential problems.

Reporter also includes alerts. Alerts are special reports that warn you about potential problems with the server’s hardware, software, or security. Alerts are automatically triggered once a predefined threshold is exceeded. For example, if the threshold value for the Excessive After-Hours Logons Alert is set to 25, the alert is triggered when 26 or more after-hours logons occur.

Report example

The Channel Usage Report shows information related to DSP channels. The report extracts any relevant information and organizes it according to the number of ingoing calls and the number of outgoing calls.


Seagate Java Viewer using Browser's JVM - Microsoft Internet Explorer provided by ...
1
of 1
75%
Preview
Applet started
Local intranet

Channel Usage Report

2/5/02 12:00:00AM - 2/6/02 12:00:00AM

Report Type : System Status

Date	Time Period	Channel Number	Incoming Calls	Outgoing Calls	Total Calls	Avg Hold Time Incoming Calls	Avg Hold Time Outgoing Calls	Erlangs
						0	0	
		Summary :	0	0	0	0	0	0
		Grand Total :				0	0	

Benefits of reports

Analyze the information in reports to help you establish a pattern of normal system behavior. As you collect reports over time, you can

- monitor system usage and system security
- assess your system’s overall efficiency
- detect potential system problems
- bill users for service usage
- identify alerts that result from possible hacker activity or potential software problems

For more information about interpreting reports, see “Interpreting reports and alerts” on page 83.

Reporter installation

Introduction

This guide assumes that CallPilot has been correctly installed and is operational. If CallPilot has not been installed, then install it before proceeding. For installation instructions, refer to the installation guide appropriate to your server type.

If the server has been installed but is not operational, refer to Part 5 of the *CallPilot Installation and Configuration* binder for information on troubleshooting your system.

Reporter is available as an installation option when you install CallPilot Manager. For instructions on installing CallPilot Manager, refer to Part 4 of the CallPilot Installation and Configuration binder.

During installation, Crystal Reports and a Sybase database are installed on the web server.

Compatibility

CallPilot Reporter 2.02 is not backwards-compatible with the CallPilot 1.07 server or client software.

Server requirements

Operating system

Reporter must be installed on a stand-alone Windows NT 4.0 or Windows 2000 web server. Reporter is not available for installation when you install CallPilot Manager on a CallPilot server.

Disk space

Reporter stores operational measurement (OM) data collected by CallPilot servers on the Reporter web-server. The amount of data that Reporter stores on the web server depends on a number of factors, including:

- the number of CallPilot servers that you use with Reporter
- the number of mailboxes stored on each CallPilot server
- the number of DSP channels in service
- the volume of traffic in your messaging system
- the database storage period defined in Reporter

If the CallPilot web server has insufficient disk space for incoming data, CallPilot servers will stop transferring to Reporter.

During Reporter software installation, the installation program calculates the amount of free space that remains on drive C. If less than 200 Mbytes of free disk space is available, the installation program displays a warning.

The 200 Mbyte limit is based on the potential database size for a single CallPilot system after several days of heavy traffic. Consider the factors listed above to assess the potential disk space consumption on your Reporter web server. You may wish to configure up to 1 GB of disk space depending on your system size. In general, the more disk space provided, the better.

For information about changing the database storage period on the Reporter web server, see “Changing the database storage period” on page 76.

ATTENTION

Reporter only checks for the amount of free disk space during the Reporter installation process.

To ensure that the CallPilot server can transfer collected OM data to Reporter, regularly monitor the amount of free disk space on the web server.

For more information about CallPilot web server requirements, refer to Part 4 of the *CallPilot Installation and Configuration* binder.

Client computers

Reporter supports the following operating systems and web browsers:

- **operating system**—Windows 98, ME, 2000, NT, and XP
- **web browsers**—Internet Explorer 5 or 6, Netscape 6.2

Support for CallPilot servers

In CallPilot 2.02, a single instance of CallPilot Reporter running on a customer-provided Web server supports up to a maximum of 20 CallPilot servers. Prior to CallPilot 2.02, CallPilot Reporter supported a maximum of only two CallPilot servers unless the performance enhancement package (PEP) CP20126G047C was installed. With this PEP installed, the maximum of 20 servers applies.

The customer-provided Web server must be a Microsoft Internet Information Server (IIS). CallPilot 2.02 supports the following IIS versions:

- IIS 4.0 on Windows NT 4.0
- IIS 5.0 on Windows 2000

Related information products

Introduction

The following CallPilot technical documents are stored on the CD-ROM that you receive with your system. The documents are also available from the following sources:

- CallPilot Manager
- My CallPilot
- the Nortel Networks Partner Information Center (PIC) at http://my.nortelnetworks.com

  You require a user ID and password to access the PIC. If you do not have a PIC account, click Register to request an account. It can take up to 72 hours to process your account request.

You can print part or all of a guide, as required.

Note: To order the documents that are available in printed format, contact your Nortel Networks sales representative.

Planning and migration guides

Use these guides before you install CallPilot to help plan your system, or to plan a migration of data from Meridian Mail to CallPilot:

Document titles	NTP number
Planning and Engineering Guide	555-7101-101
Installation and Configuration Planner	not applicable
Meridian Mail to CallPilot Migration Utility Guide	555-7101-801

Installation and configuration guides

The following guides describe how to install the following:

- CallPilot server hardware and software
- desktop messaging and My CallPilot software

Document titles	NTP number
Desktop Messaging Installation Guide	555-7101-505
Installation and Configuration Guide for your server model This is a binder that contains the following five documents: ▪ *Part 1: Installation and Maintenance Overview* ▪ *Part 2: <Server model> Server Hardware Installation* ▪ *Part 3: <Switch name> and CallPilot Server Configuration* ▪ *Part 4: Software Installation and Maintenance* ▪ *Part 5: <Server model> Server Maintenance and Diagnostics*	Refer to your binder for your NTP numbers.

Administration guides

The following guides provide specialized information to help you configure CallPilot, administer and maintain it, and use its features:

Document titles	NTP number
Administrator's Guide	555-7101-301
Reporter Guide	555-7101-310
Application Builder Guide	555-7101-325

Document titles	NTP number
Desktop Messaging Administration and Maintenance Guide	555-7101-503

Networking guides

The following guides describe how to plan, install, set up, and troubleshoot the CallPilot networking services:

Document titles	CallPilot release	NTP number
Networking Enhancements Guide	2.02	555-7101-507
Networking Planning Guide	2.02	555-7101-100
NMS Implementation and Administration Guide	2.02	555-7101-302
AMIS Networking Implementation and Administration Guide	2.02	555-7101-303
Enterprise Networking Implementation and Administration Guide	2.02	555-7101-304
Integrated AMIS Networking Implementation and Administration Guide	2.02	555-7101-305
VPIM Implementation and Administration Guide	2.02	555-7101-306

Note: The CallPilot networking guides remain mostly unchanged since CallPilot 1.0.

End user guides

The following guides are intended for CallPilot end users, such as phoneset users and desktop messaging users:

Document titles
Unified Messaging What's New Card
Unified Messaging Quick Reference Card
Unified Messaging Wallet Card
Menu Interface Quick Reference Card
Alternate Command Interface Quick Reference Card
Command Comparison Cards
Multimedia Messaging User Guide
Speech Activated Messaging User Guide
Desktop Messaging User Guides
My CallPilot User Guide
E-mail Notification User Guide

Troubleshooting

The *CallPilot Troubleshooting Reference* describes symptoms that can appear on all CallPilot server platforms, and describes ways to resolve them.

The *CallPilot Troubleshooting Reference* is written for Nortel Networks distributors and technical support representatives; therefore, it is not part of the customer documentation package. It is continually being updated by Nortel Networks and is available from the Nortel Networks Partner Information Center (PIC) at http://my.nortelnetworks.com.

You require a user ID and password to access the PIC. If you do not have a PIC account, click Register to request an account. It can take up to 72 hours to process your account request.

Note: If you are not a Nortel Networks distributor, then contact your Nortel Networks technical support representative for assistance.

Using online sources

CallPilot administration online Help

The CallPilot Manager and CallPilot Reporter software contain administration online Help areas that provide access to

- technical documentation in Acrobat PDF format
- online Help topics in HTML format

To access online information, use either of the following methods:

- Click the orange Help button at the top of any page to access the Administration Help area.
- Click the grey Help button on any page to display a topic that relates to the contents of the page.

For more information about using these Help systems, access the CallPilot Manager Help, open the Getting Started book, and click “Navigating CallPIlot Manager Help”

The Application Builder software contains a Windows Help system as well as context-sensitive Help (available by clicking the ? button and then a field or label).

CallPilot end user online Help

The My CallPilot software contains a Useful Information area that provides access to the end-user guides in HTML format. Online user guides in Acrobat PDF format are also available from the Useful Information online Help.

To access online Help for the currently selected My CallPilot tab, click the Help button on the upper-right corner of the My CallPilot page.

Desktop messaging provides product-specific Windows Help for groupware clients (Microsoft Outlook, Novell GroupWise, and Lotus Notes). The stand-alone version of CallPilot Player also provides addressing and troubleshooting information for Internet mail clients.

Contacting technical support

Contact your distributor’s technical support organization to get help with troubleshooting your system.

Contacting Nortel Networks

If you have comments or suggestions for improving CallPilot and its documentation, contact Nortel Networks at the following web site address:

http://www.nortelnetworks.com/callpilot_feedback

Chapter 2

Using reports and alerts

In this chapter

Section A: Starting and exiting CallPilot Reporter

In this section

Starting CallPilot Reporter

To start CallPilot Reporter

1 Start CallPilot Reporter in either of the following two ways:

- If you are logged on to CallPilot Manager, choose Tools → Reporter or
- Type the URL ’http://<report-server>/cpmgr/cprpt’ for CallPilot Reporter in the Address field of your web browser, and then press Enter.

2 On the CallPilot Manager logon page, specify the logon information.

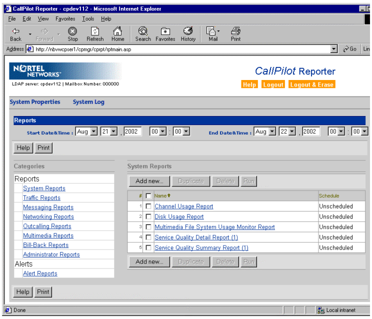
a. Type your mailbox number and password

b. Specify the computer name or IP address of the CallPilot server you want to access

c. Click Login.

Tip: You can create a shortcut on your desktop to access the CallPilot Logon dialog box quickly. For more information, see the online Help.

The CallPilot Reporter page


CallPilot Reporter - cpdev112 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Go Lin
NORTEL NETWORKS
CallPilot Reporter
Help Logout Logout & Erase
System Properties System Log
Reports
Help Print
Categories
System Reports
Add new... Duplicate Delete Run
Done
Local intranet

Address: http://nbvwcpser1/cpmgr/cprpt/rptmain.asp

LDAP server: cpdev112 | Mailbox Number: 000000

Start Date&Time : Aug 21 , 2002 00 : 00 End Date&Time : Aug 22 , 2002 00 : 00

Reports
- System Reports
- Traffic Reports
- Messaging Reports
- Networking Reports
- Outcalling Reports
- Multimedia Reports
- Bill-Back Reports
- Administrator Reports

Alerts
- Alert Reports

#	□	Name	Schedule
1	□	Channel Usage Report	Unscheduled
2	□	Disk Usage Report	Unscheduled
3	□	Multimedia File System Usage Monitor Report	Unscheduled
4	□	Service Quality Detail Report (1)	Unscheduled
5	□	Service Quality Summary Report (1)	Unscheduled

Reports are divided into categories. To display reports in a category, click on the category name.

The report list shows the available reports in the selected category and whether they are scheduled to run.

To confirm a first-time connection to a CallPilot server

1 Once you successfully log on to Reporter, click System Log.

2 Look for the message “Connection to CallPilot Server” in the log.

- If the message appears, your connection to CallPilot was successful.
- If an error occurs, click Logout & Erase to delete the Reporter profile and try to log on again. If Reporter still cannot connect to CallPilot, ensure that the network connection between the standalone web server and CallPilot is working, and then try to logon again.

Note: The message “Connection to CallPilot Server” only appears in the System Log the first time an administrator logs on to a CallPilot system. If there is a subsequent successful logon by another administrator, the message does not appear in that administrator's System Log.

To display a list of reports or alerts

1 If it is not already open, choose Tools → Reporter to open CallPilot Reporter.

Result: The Report or Alert categories are listed.

2 In the Categories section, click the appropriate report category. For example, to find the System Traffic Summary Report, click Traffic Reports.

To view the list of Alerts, click Alert Reports.

Result: The list of reports in that category appears on the right side of the page.

Exiting CallPilot Reporter

Introduction

There are two ways to exit Reporter:

- Exit and save your profile—Save your Reporter settings and custom reports for future use when you log off.
- Exit and remove your profile—Remove all custom settings and reports when you log off.

Note: If you are the last person with settings and reports stored on this system and you remove your profile, then all Operational Measurements (OM) data and scheduled cleanup jobs are deleted. The first time a new user logs on to Reporter for the CallPilot system, OM data collection restarts automatically.

For more information about profiles, see “Reporter profiles” on page 74.

To exit Reporter and save your profile

On the CallPilot Reporter page, click Logout.

To exit Reporter and remove your profile

1 On the CallPilot Reporter page, click Logout & Erase.

Result: A confirmation message asks if you are sure you want to remove this system.

2 Click Yes.

Result: Reporter ends the session and deletes all custom reports and custom settings.

The next time you log on to Reporter, a new profile is created for you.

Note: If there is any change in Computer Name of the CallPilot that Reporter is connecting to, please remove the profile from Reporter prior to the changes by clicking ’Logout & Erase’ and reconnect again after the change is made. This action is required if the connecting CallPilot is completly removed from the network.

Section B: Creating reports and alerts

In this section

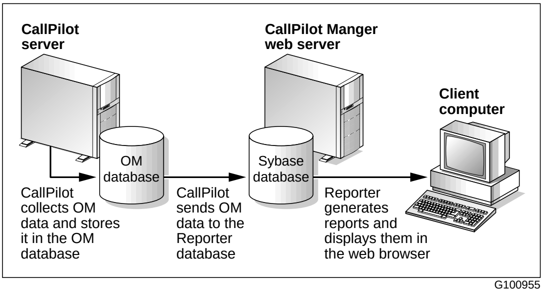
Enabling data collection

Introduction

Operational measurements (OM) data is used for reporting system activity and usage. Many activities within a CallPilot system generate operational measurements that you can review, monitor, and evaluate with Reporter.

Data collection in CallPilot Reporter

The diagram below shows how OM data is collected, stored, and displayed:


CallPilot server
CallPilot Manger web server
Client computer
OM database
Sybase database
CallPilot collects OM data and stores it in the OM database
CallPilot sends OM data to the Reporter database
Reporter generates reports and displays them in the web browser
G100955

Data collection on the OM server

To generate reports, OM data collection must be enabled on the CallPilot server. The CallPilot server collects OM data and stores it in its OM server along with summary information at one-hour intervals.

You can turn OM data collection on or off in CallPilot Manager and store collected data on the OM server for up to 10 days.

Data collection on the Reporter web server

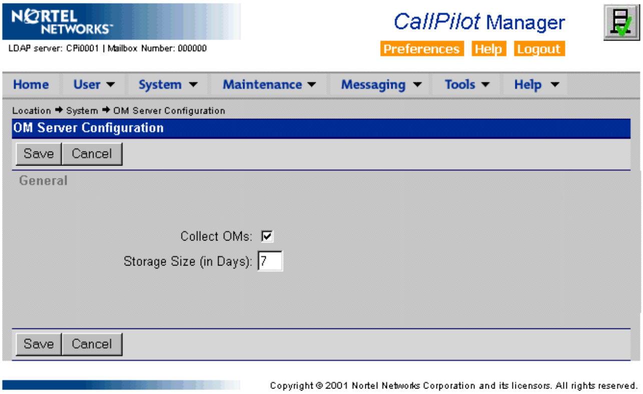
The first time an administrator connects to a CallPilot server with Reporter, Reporter begins receiving OM data for that CallPilot server and stores it in the Reporter database. Reporter continues storing OM data for a CallPilot server as long as a profile exists for the server. For more information about profiles, see “Reporter profiles” on page 74.

The storage period for the Reporter database is configured in Reporter. Access to Reporter administration tasks depends on your administrative privileges. For more information, see Chapter 3, “Administration tasks.”

To enable OM data collection

1 In CallPilot Manager, click System → OM Configuration.

Result: The OM Configuration page appears.



LDAP server: CPi0001 | Mailbox Number: 000000

Location ➔ System ➔ OM Server Configuration

OM Server Configuration

Collect OMs: ☑

Storage Size (in Days): 7

Copyright © 2001 Nortel Networks Corporation and its licensors. All rights reserved.

2 Check the Collect OMs box to enable OM data collection.

3 In the Storage Size (in Days) box, type the number of days to store data on the OM server.

4 Click Save.

Adding reports and alerts to the report list

Introduction

To view, print, or export a report, it must appear in the CallPilot report list. To help you get started, ten reports and six alerts that are used on a regular basis appear in the various Report Categories. If you require additional reports in any category, you can add them to the report list.

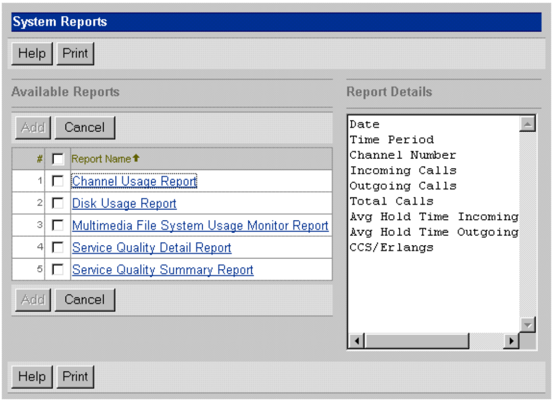
To add reports and alerts to the CallPilot Reporter window

1 In Reporter, in the Categories section, click the type of report you want to add.

2 Click Add New.

3 Click the check boxes beside the reports you want to add.

Tip: To see what information the report contains in the report, click the name of the report. The report details appear to the right.



#	□	Report Name
1	□	Channel Usage Report
2	□	Disk Usage Report
3	□	Multimedia File System Usage Monitor Report
4	□	Service Quality Detail Report
5	□	Service Quality Summary Report

```
Date
Time Period
Channel Number
Incoming Calls
Outgoing Calls
Total Calls
Avg Hold Time Incoming
Avg Hold Time Outgoing
CCS/Erlangs
```

4 Click Add.

5 Click OK to respond to the confirmation message.

If you add a report that already appears in the report list, CallPilot Reporter assigns a number to the duplicate report name and adds it to the list. For example, if you add a copy of the Channel Usage Report, a copy of the report, named Channel Usage Report (2), appears in the list.

6 To change the default name, click the name in the report list.

7 In the Properties window, General Settings, change the name in the Report Name box.

8 In the Comments box, type any additional information about the report.

9 Click Save.

Result: You can now run, print, or customize the report.

Removing reports and alerts from the list

Introduction

If you seldom use a report or alert, you can remove it from the CallPilot report list. This ensures that your display does not become cluttered with unused reports.

Example

During the last two months, you have used the Fax Delivery Report to monitor fax transmission errors. However, the fax problem has now been solved and you no longer need this report.

What happens when you remove a report or alert

When you remove a report or alert, you delete the report from the report list on the CallPilot Reporter main page and cancel the report’s print schedule. However, a permanent copy of the original report remains on the Add New page. This means that you can add the report to the report list in the future.

Note: Duplicated reports are deleted permanently from the CallPilot Reporter program.

To remove a report or alert

1. Display the list of reports in the appropriate report category.
2. In the report list, click the check box beside the reports you want to remove.

   Note: To select all reports, click the check box in the header row of the list. To deselect all reports, click the header row again.
3. Click Delete.

   Result: A confirmation dialog box appears.
4. Click Yes to confirm the deletion.

Duplicating a report or alert

Introduction

You can create a new report or alert based on an existing report, and then customize it to suit your needs.

Example

The Inactive Users Report shows which users are not responding to their voice mail. If you want to monitor inactive users by department, you can make several copies of the report, and then apply filters to each copy of the report to show only inactive users from one department. For example, you can create the Inactive Users/Accounting Report to show users in the accounting department who are not using their voice mail, and the Inactive Users/Human Resources Report to show users in the human resources department who are not using their voice mail.

To create a report from an existing report or alert

1. Display the list of reports in the appropriate report category.
2. In the report list, click the check box beside the report that you want to use as the basis for the new report.
3. Click Duplicate.

   Result: Reporter automatically assigns a number to the duplicate report name and adds the report to the CallPilot Reporter list. For example, if you duplicate the Channel Usage Report, a copy of the report, named Channel Usage Report (2), appears in the list.
4. To change the default name, click the name of the duplicated report in the report list.
5. In the Properties window, General Settings, change the name in the Report Name box.

6 If desired, in the Comments box, type details about the report.

7 Select filtering criteria (see page 52) and sorting criteria (see page 50)

8 Click Save.

Section C: Viewing reports and alerts

In this section

Viewing a report or alert

Introduction

You can generate a report and view it on the screen at any time.

Before you view a report on the screen, specify the number of days of data that you want the report to contain. For example, you can set the report to display data for three days—Monday, Tuesday, and Wednesday. Set up the report to collect data from Monday at 12:00 a.m. to Wednesday at 12:00 p.m.

Tips

Here are some useful tips for viewing reports:

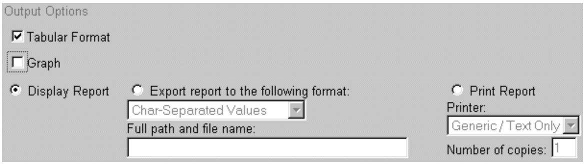
- To increase or decrease the size of the report, click the size percentage field at the top of the window.
- To scroll through the pages one at a time, use the left and right arrow buttons.
- To print the report, click the printer icon. For more information on printing reports, see Section E: “Printing and exporting reports and alerts,” on page 57.

To view a report or alert

1. Display the list of reports in the appropriate report category.
2. Click the name of the report you want to view.

   Result: The Properties window for that report appears.

3 Scroll down to the Output Options section.



Output Options

☑ Tabular Format

□ Graph

● Display Report

○ Export report to the following format: Char-Separated Values

Full path and file name:

○ Print Report

Printer: Generic / Text Only

Number of copies: 1

4 Select the format for the report (Tabular and/or Graph). You can select a single format or both formats.

Note: Not all reports support the Graph option.

5 Click Save.

6 On the CallPilot Reporter page, in the Start Date & Time boxes, select the first date and time for the data included in the report (for example, Feb 14 2001, 14:00).

Note: The time boxes use the 24-hour clock.

7 In the End Date & Time boxes, select the last date and time for data included in the report.

8 In the report list, click the check box beside the report you want to view.

9 Click Run.

Result: The selected report appears.

Note: Viewing a report or alert only works in on-demand basis. Although ’Export Report’ or ’Print Report’ can be selected for schedule exporting and schedule printing, by clicking Run will always display the report or alert on the screen. ’Export Report’ and ’Print Report’ options are designed only for schedule exporting/printing and when alert is triggered.

Checking alert status

Introduction

When an alert is triggered, the Triggered column displays the date when the alert was triggered.

Reporter updates the status of the alert each time it performs an alert check.

- If the collected data still exceeds the alert threshold, Reporter updates the date in the Triggered column.
- If the collected data no longer exceeds the alert threshold, Reporter clears the alert.

To maintain a record of the alert over time, you can schedule the alert to print or export alert data when the alert is triggered. For more information, see “Printing or exporting alerts when they are triggered” on page 64.

To view alert status

Select the Alert Reports category in the Categories list.

Section D: Customizing reports and alerts

In this section

Overview of customization

Introduction

When you customize a report or alert, you can eliminate excessive data and organize the remaining information into an easy-to-read format. Well-organized reports improve the speed and accuracy with which you interpret data.

Note: You can customize only the data contained in a report. The fields in a report are predefined and cannot be changed.

How reports and alerts can be customized

There are various ways to customize a report or alert as shown in the following table:

	Reports	Alerts
■ add comments	✔	✔
■ sort	✔	✔
■ filter	✔	
■ set a threshold		✔

Adding comments

Adding comments lets you specify additional information about the data.

Sorting

Sorting organizes the data in a report so that relevant information is grouped together. This makes it easier to analyze and interpret information.

Filtering

Filtering reduces the volume of data displayed in a report. For example, instead of showing data for all users, you can use filtering to select data for users in only one department.

Setting a threshold for an alert

Setting a threshold for an alert allows you to specify the number of events that must occur before the alert is triggered.

Adding comments to reports or alerts

Introduction

When you add comments to the data in a report, you ensure that additional information is not forgotten or overlooked.

Limitations

Comments are visible only on the screen. They do not appear when the report is printed.

To add comments to a report

1. Display the list of reports in the appropriate report category.
2. Click the name of the report to which you want to add comments.

   Result: The Properties window for that report appears.
3. In the General Settings type any additional information about the report in the Comments box.
4. Click Save.

Sorting the data in reports or alerts

Introduction

You can sort the data in a report to ensure that relevant information is grouped together. This makes it easier to analyze and interpret information.

Example

The Inactive User Report shows all users who are not accessing their mailboxes. Use the sorting feature to group users by mailbox instead of name.

Limitations

Some reports cannot be sorted. In the Properties window, if the Sorting section does not appear after the General Settings section, you cannot sort the report. Also, not all items on the Report can be sorted.

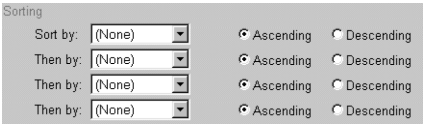
To sort the data contained in a report or alert

1 Display the list of reports in the appropriate report category.

2 Click the name of the report you want to sort.

Result: The Properties window for that report appears.

3 In the Sorting section, select the sort criteria in the Sort by lists.



Sorting

Sort by: (None) ● Ascending ○ Descending

Then by: (None) ● Ascending ○ Descending

Then by: (None) ● Ascending ○ Descending

Then by: (None) ● Ascending ○ Descending

By default the data is sorted in ascending order. To reverse the order, click Descending. You can specify up to four sort criteria. Each additional criterion sorts within the previous criterion.

4 Click Save.

Filtering data in reports

Introduction

When you filter data, you limit the scope of the data in a selected report. For example, if you set the selection criteria for the Messaging Usage Bill-back Report to include a particular department, the resulting report contains only data for that department.

Limitation

Some reports cannot be filtered. If the Selection Criteria section does not appear in the Properties window, then the report cannot be filtered.

Filtering

Before you can filter data, you must define your selection criteria. There are three types of selection criteria—item, operator, and value.

Item

The item is the main criterion that Reporter uses to filter data. Each report has its own items, which are displayed in the Item list box. For example, the items listed in the Top Users of Storage Report are Mailbox Class, and Switch location.

Operator

The operator is a mathematical function that compares the item with the value. Seven possible operators can be used to define your criteria:

- equal to
- not equal to
- greater than
- less than

- greater than or equal to
- less than or equal to
- is like

Value

The value specifies a range for the criterion chosen from the Item list. The information entered in this box depends on the item you select. For example, if you select Name as the item, the value must be a user’s name. If you select Department, the value must be the department’s name.

Using wildcard characters

If you use the “is like” operator, then you can use wildcard characters in your filter value.

You can use the asterisk (*) to represent multiple characters. For example, in the Top Users of Storage report, if you want to include only those users whose names start with “Ma”, select Name as the item, Is Like as the operator and type **Ma*** as the value.

You can also use the question mark (?) to represent a single character. For example, if you want a report to include all mailboxes in the range 4350 to 4359, use the filter value 435?.

Filtering example

The Top Users of Storage Report helps you determine which mailbox owners are using the most voice storage. To reduce the scope of the data displayed in this report, select Mailbox Class as the item, “is equal to” as the operator, and Regular Users as the value. Together these selection criteria produce a report that shows only the top users of storage in the Regular Users Class.

Narrowing and broadening the filter's scope

If you want to further reduce the volume of information in a report, select All conditions. This ensures that the information in the report meets all of the criteria you specified.

If you want to increase the volume of information in a report, select At least one condition. This ensures that the information in the report meets at least one of the criteria you have specified.

To filter a report's data

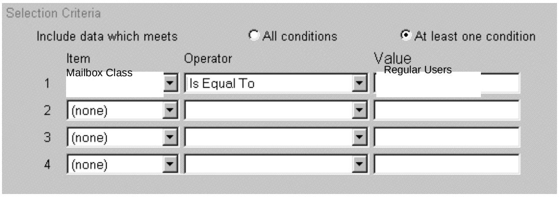
1 Display the list of reports in the appropriate report category.

2 Click the name of the report you want to filter.

Result: The Properties window for that report appears.

3 Look for the Selection Criteria section.

Note: If the Selection Criteria section of the Properties window does not appear, this report cannot be filtered.



Selection Criteria

Include data which meets ○ All conditions ● At least one condition

	Item	Operator	Value
1	Mailbox Class	Is Equal To	Regular Users
2	(none)		
3	(none)		
4	(none)		

4 In the Item list box, select a condition.

5 In the Operator list box, select how the item you selected will be compared with the value (for example, equal to or not equal to).

6 In the Value box, type an appropriate value.

7 If desired, repeat steps 4 to 6 in the next three rows.

8 Do one of the following:

- To narrow the scope of the filter, click All conditions.
- To widen the scope of the filter, click At least one condition.

9 Click Save.

Setting a threshold for an alert

Introduction

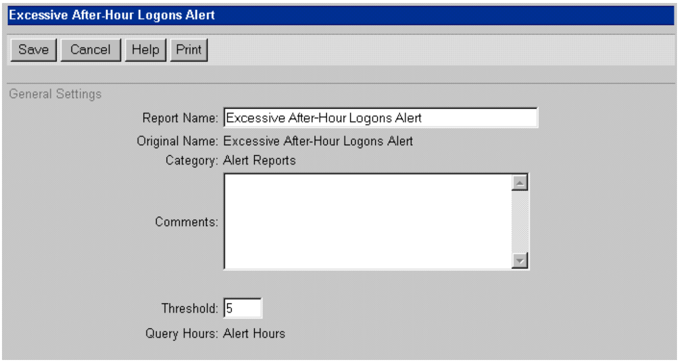
For certain events such, as a failed logon, the system compares the number of these events to a predefined limit or “threshold.” Whenever the threshold value is exceeded, the alert is triggered. For example, if the threshold value for the Excessive After-Hours Logons Alert is set to 25, the alert is triggered when 26 or more after-hours logons occur.

To set the threshold for an alert

1 Display the list of alerts.

2 Click the name of the alert for which you want to set the threshold.

Result: The Properties window for the alert appears.



Report Name: Excessive After-Hour Logons Alert
Original Name: Excessive After-Hour Logons Alert
Category: Alert Reports
Comments:
Threshold: 5
Query Hours: Alert Hours

3 In the General Settings section, type the maximum number of occurrences before the alert is triggered in the Threshold box.

4 Click Save.

Section E: Printing and exporting reports and alerts

In this section

Overview of printing and exporting

Introduction

When you generate reports or alerts over a period of time, you can identify significant patterns and trends related to system usage.

Example

You have scheduled the Inactive User Report to print out once a day for three months. At the end of the first month, you analyze the reports and notice that three users have never logged on to their mailboxes. You may want to ensure that these users are properly trained to use the voice mail system.

Printing and exporting options

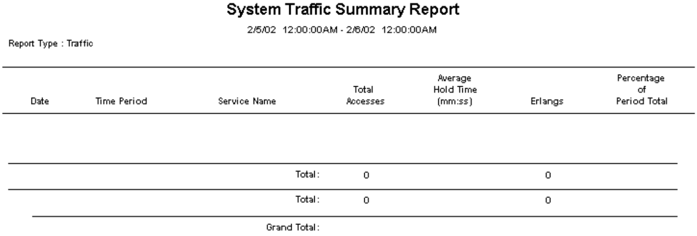
You can print or export reports and alerts on a regular basis according to a preset schedule, or you can print or export reports on demand. Storage of reports over a period of time helps you to identify patterns and trends related to system usage.

You can only schedule reports for printing or exporting on the Reporter web server. To print or export reports on a client computer, you can print or export the report on demand.

Most of the reports generated by Reporter are printed in a standard table format. However, you can print some reports as graphs. Graphs let you analyze data quickly, observe trends, and make comparisons about system usage.

Example

The System Traffic Summary Report lets you monitor the total amount of traffic processed by the different services installed on your system. You can print this report as a graph to make it easy to identify the system's busiest hours and to determine whether you have sufficient channel capacity to handle the volume of traffic.



System Traffic Summary Report

2/5/02 12:00:00AM - 2/6/02 12:00:00AM

Report Type : Traffic

Date	Time Period	Service Name	Total Accesses	Average Hold Time (mm:ss)	Erlangs	Percentage of Period Total
		Total :	0		0	
		Total :	0		0	
		Grand Total :				

Export formats

When you export a report or alert, you change its current file format to the file format of an external program. Use exporting if you want to view the data in an external program, such as a spreadsheet. The export feature is especially useful when you need to transfer data from bill-back reports to an external billing program.

The file formats to which reports can be exported include the following:

File format	Extension
Comma-separated values, Character-separated values	CSV
Crystal Reports 7, 8	RPT
Data Interchange Format	DIF
Excel 5.0, 5.0 tabular, 7.0, 7.0 tabular, 8.0, 8.0 tabular	XLS

File format	Extension
HTML 32, 4.0 Standard	HTML
Lotus 1-2-3	1A 2.x 3.x
Portable Document Format	PDF
Lotus 1-2-3	WK1, WK2, WK3
Record style (columns of values)	REC
Rich Text Format	RTF
Tab-separated text	TTX
Tab-separated values	TSV
Text	TXT
Word for Windows	DOC

Limitations

When you export a report, some or all of the formatting may be lost or modified.

Printing or exporting based on a schedule

Introduction

When you set up a schedule, you can print or export standard reports on a daily, weekly, or monthly basis. Generate reports on a regular basis to help you identify patterns and trends related to system usage.

Scheduled reports print to a specified printer connected to your web server. You must set up the CallPilot Reporter service on the web server to support scheduled printing.

If you want to print a report with a printer configured on your client computer, you can print the report on demand. For more information, see “Printing or exporting on demand” on page 65.

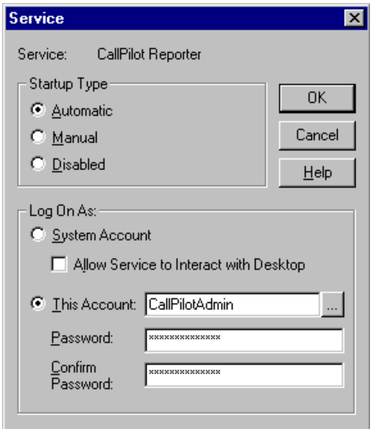
Tip: Store printed reports so that you can identify and compare trends over a period of time. If you discard reports too soon, significant problems can go unnoticed.

You cannot schedule alerts, but you can set up an alert to print or export data when it is triggered. For more information, see “Printing or exporting alerts when they are triggered” on page 64.

To set up the CallPilot Reporter service for printing

1. On the Reporter web server, open the Windows Control Panel.
2. Open the Services applet. The Services window appears.

3 In the list of services, select CallPilot Reporter, and then click Startup. The Service window appears.



Service: CallPilot Reporter

Startup Type

● Automatic

○ Manual

○ Disabled

Log On As:

○ System Account

□ Allow Service to Interact with Desktop

● This Account: CallPilotAdmin

Password: **************

Confirm Password: **************

4 In the Log On As section, select This Account, and then specify a user account with the appropriate access privileges.

- To print on a network printer, specify a user account with network access privileges.
- To print on a local printer connected to the web server, specify a user account with local access privileges.

5 Click OK.

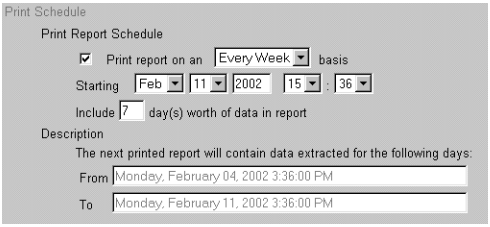
To set a schedule for a report

1 Display the list of reports in the appropriate report category.

2 Click the name of the report you want to schedule.

Result: The Properties window for that report appears.

3. Scroll down to the Print Schedule section.



Print Schedule

Print Report Schedule

☑ Print report on an Every Week basis

Starting Feb 11 2002 15 : 36

Include 7 day(s) worth of data in report

Description

The next printed report will contain data extracted for the following days:

From Monday, February 04, 2002 3:36:00 PM

To Monday, February 11, 2002 3:36:00 PM

4. Make sure that the Print report on an...basis box is checked.
5. From the Print report on an... basis list, specify how often you want to print or export the report (every day, week, or month).

   Note: Reports scheduled on a monthly basis print or export data on the first day of the month.
6. In the Starting row, specify when you want the report to print the first time.

   Result: The Include... day(s) worth of data in report box shows the number of days of data included in the report. For example, if you set the report to print weekly, seven days of data are automatically included in the report.
7. Check the Description section. The From and To boxes show the date and time for which the next printed report will contain data.
8. In the Output Options section, select the required options:
   - To print the report, select Print Report.
   - To export the report, select Export report to the following format. Select a format from the list, and then specify the path and file name for the file (for example, d:\reports\exported). If the appropriate file extension is not provided, ensure that you type the correct file extension.
9. Specify the format for the report (Tabular and/or Graph). You can print scheduled reports in graph format, but you cannot export them in graph format.
10. Click Save.

Printing or exporting alerts when they are triggered

Introduction

Since alerts are not a part of day-to-day system operation, you cannot schedule printing and data export of alerts. Instead, when you choose to print or export an alert, Reporter prints or exports the data when the alert is triggered.

You can print alerts on any printer connected to the web server on which Reporter is installed. You must set up the CallPilot Reporter service on the web server to support printing of triggered alerts. For details about setting up the CallPilot Reporter service, see “To set up the CallPilot Reporter service for printing” on page 61.

You can export data to any network location that is always accessible to the web server on which Reporter is installed.

To print or export an alert when it is triggered

1. In the list of alerts, click the name of the appropriate alert.

   Result: The Properties window for the alert appears.

2. Locate the Output Options section.
3. In the Output Options section, select the required options:
   - To print the report, select Print Report.
   - To export the report, select Export report to the following format. Select a format from the list, and then specify the path and file name for the file.
4. Type the full path and filename to which the data will be exported.
5. Click Save.

Printing or exporting on demand

Introduction

Print or export a report on demand when you do not want to wait for a scheduled report to execute. You can also print a report on demand if you suspect that there is a problem with your system and you require data ahead of the schedule.

When you run a report on demand, you can print it to any printer that is configured on the client computer. You can only print scheduled reports on a printer configured on the Reporter web server.

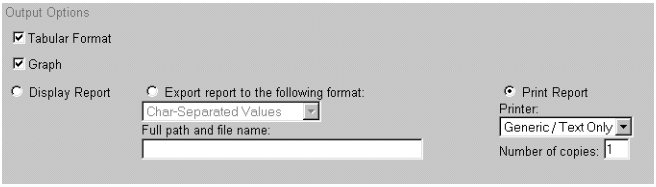
To print data on demand

1 Display the list of reports in the appropriate report category.

2 Click the name of the required report.

Result: The Properties window for that report appears.

3 In the Output Options section, specify the format for the report (Tabular and/or Graph).



Output Options

☑ Tabular Format

☑ Graph

○ Display Report

○ Export report to the following format: Char-Separated Values

Full path and file name:

● Print Report

Printer: Generic / Text Only

Number of copies: 1

4 Click Save.

5 Above the report list, in the Start Date & Time boxes, select the start date and time for the data included in the report.

6 In the End Date & Time boxes, select the end date and time for the data included in the report.

7 In the report list, select the check box beside the name of the report you want to print or export.

8 Click Run. The report appears on the screen in a separate window.

9 Click the Print button on the toolbar. The Print dialog box appears.

10 Select the printer to use and the number of copies, and then click OK.

11 Close the report window when you are finished.

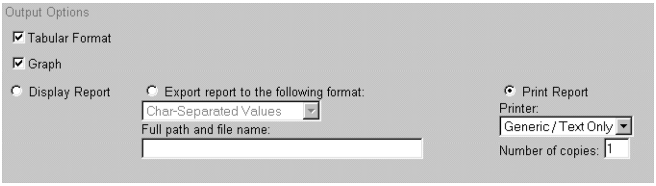
To export data on demand

1 Display the list of reports in the appropriate report category.

2 Click the name of the required report.

Result: The Properties window for that report appears.

3 In the Output Options section, specify the format for the report (Tabular and/or Graph).



Output Options

☑ Tabular Format

☑ Graph

○ Display Report

○ Export report to the following format: Char-Separated Values

Full path and file name:

● Print Report

Printer: Generic / Text Only

Number of copies: 1

4 Click Save.

5 Above the report list, in the Start Date & Time boxes, select the start date and time for the data included in the report.

6 In the End Date & Time boxes, select the end date and time for the data included in the report.

7 In the report list, select the check box beside the name of the report you want to print or export.

8 Click Run. The report appears on the screen in a separate window.

9 Click the File Export button on the toolbar. The Export dialog box appears.

10 Select the export file format and destination path, and then click OK.

11 Close the report window when you are finished.

Printing or viewing reports as graphs

Introduction

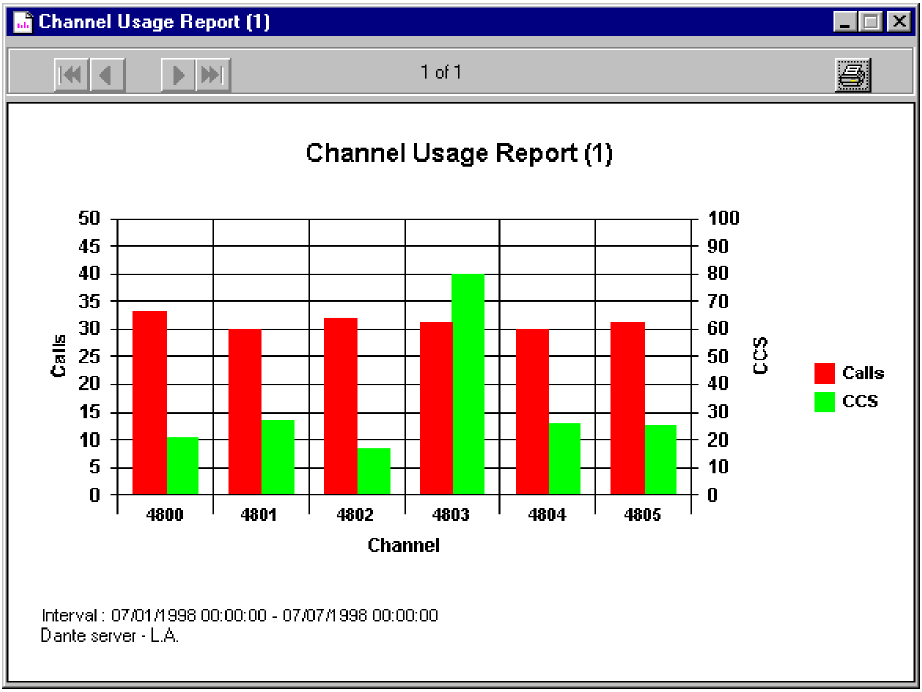
Most of the reports generated by Reporter are printed as tables. However, you can print some reports as graphs. Graphs let you analyze data quickly, observe trends, and make comparisons about system usage.

Scheduled reports print to a specified printer connected to your web server. When you run a report on demand, you can print it to any printer that is configured on the client computer.

Reports that are available as graphs

You can view or print the following reports as graphs:

- Building Block Summary Report
- Networking Activity Report
- Fax Deliveries Activity Report
- Channel Usage Report
- Multimedia File Usage Monitor Report
- Disk Usage Report
- System Traffic Summary Report

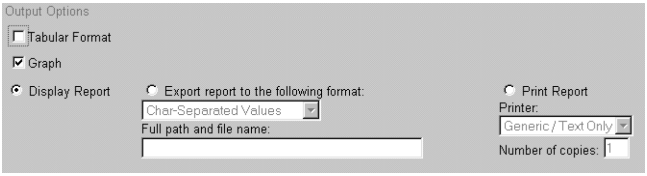


Interval : 07/01/1998 00:00:00 - 07/07/1998 00:00:00
Dante server - L.A.

To print or view a report as a graph

1. Display the list of reports in the appropriate report category.
2. Click the name of the report you want to schedule.

   Result: The Properties window for that report appears.
3. Scroll down to the Output Options section.



Output Options

□ Tabular Format

☑ Graph

● Display Report

○ Export report to the following format: Char-Separated Values

Full path and file name:

○ Print Report

Printer: Generic / Text Only

Number of copies: 1

4. Select Print Report or Display Report.

5. Click the Graph check box.

   Note: To view these reports in regular report format, ensure that the Tabular Format box is checked.

6. Click Save.

Printing a list of reports or alerts

Introduction

If you want to keep a list of reports or alerts for future reference, print the contents of the Reporter window. You can print the list on any printer configured on the client computer.

To print a list of reports or alerts

1. Display the list of reports in the appropriate report category.
2. Click Print.

   Result: The Print dialog box appears.
3. Click OK.

Chapter 3

Administration tasks

In this chapter

Overview

Introduction

Administration options for Reporter are available in the Reporter Main, System Properties, and System Log windows. The CallPilot Reporter administration tasks include the following:

- changing the database storage period (System Properties window)
- backing up the database (Sybase)
- changing the alert hours (System Properties window)
- changing the traffic units (System Properties window)
- viewing the System Log (System Log window)
- removing a system (Reporter Main window)

Reporter profiles

The first time you log on to Reporter, a new profile is created for you. Your profile includes

- all custom reports that you created
- your Reporter settings
- your Reporter log

When you are finished your Reporter session, you can

- exit Reporter and save your profile (Logout)
- exit Reporter and remove your profile (Logout & Erase)

Saving your profile

If you save your profile, your custom settings and custom reports are available the next time you log on to Reporter. Your custom reports are only available to you.

If you want to share specific custom reports with other users, consider creating a mailbox specifically for accessing shared reports. All administrators with access to Reporter can use the mailbox number and password to log on to Reporter and access shared reports.

Removing your profile

If you remove your profile, Reporter deletes all custom reports and custom settings. Reporter creates a new profile for you with the default settings and reports the next time you log on.

Profiles and data collection

The first time an administrator connects to a CallPilot server with Reporter, Reporter creates a profile for the administrator and begins receiving and storing OM data for the CallPilot server. Since the administrator owns the first profile, the administrator’s Reporter log contains some information that will not appear in subsequent profiles created for the same CallPilot server, including

- the message "Connection to CallPilot Server" for a successful first-time connection to a CallPilot system
- information about nightly audits

If the administrator removes his or her profile, the nightly audit information is transferred to the next available profile.

Reporter continues to collect OM data for a CallPilot server as long as a profile exists that is associated with the server. If you remove your profile, and you are the last person with a profile associated with the server, Reporter performs the following actions:

- Reporter stops OM data collection for the CallPilot server.
- Reporter deletes all OM data and scheduled cleanup jobs associated with the CallPilot server from the Reporter database

Changing the database storage period

Introduction

CallPilot collects operational measurements (OM) data on the OM server. Reporter then retrieves the data and stores it in the Reporter database. By default, data is stored in the OM database for 30 days. You can specify a storage period of up to 120 days for the Reporter database.

Notes:

- To change the Reporter database storage period, you must have Reporter Administration privileges.
- Since the storage period specified by other administrators may be different, Reporter uses the maximum value specified in a profile associated with the CallPilot server. For more information about profiles, see “Reporter profiles” on page 74.

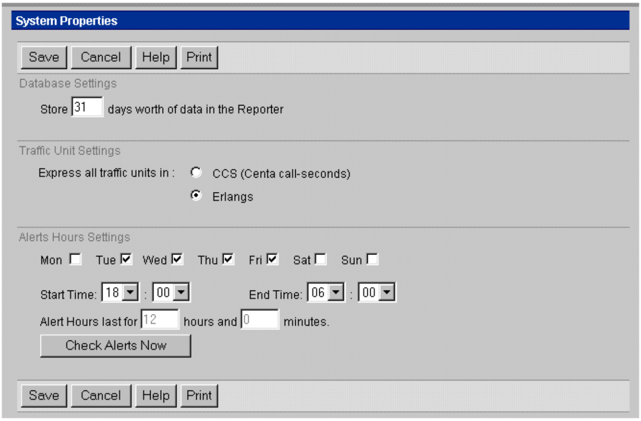
ATTENTION

If you specify 0 for the Reporter database storage period, all of the data for the system that you are logged on to is deleted from the OM database during the next nightly audit.

To change the storage period for the Reporter database

1 On the CallPilot Reporter page, click System Properties.

Result: The System Properties window opens.



Database Settings

Store 31 days worth of data in the Reporter

Traffic Unit Settings

Express all traffic units in : ○ CCS (Centa call-seconds) ● Erlangs

Alerts Hours Settings

Mon □ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat □ Sun □

Start Time: 18 : 00 End Time: 06 : 00

Alert Hours last for 12 hours and 0 minutes.

2 In the Database Settings section, type the number of days to store data in the Reporter database.

3 Click Save.

4 If you entered 0 as a value, the system will delete all data for .the current CallPilot system during the next nightly audit.

Backing up the database

Introduction

To prevent data from being lost due to a system failure, back up your database regularly.

Reporter uses a Sybase database to store collected OM data. To back up your Reporter database, consult your Sybase documentation.

Changing the alert hours

Introduction

If you want to be notified of potential hacking that takes place outside of regular business hours, you can set or change the hours during which the monitoring takes place. Information is recorded in the following reports:

- Excessive After-Hours Logons Alert
- Excessive Thru-Dialer Access Alert

Note: By default, Monday to Friday from 6:00 p.m. to 6:00 a.m. the following morning, and all day Saturday and Sunday are already selected.

To change the alert hours

1. On the CallPilot Reporter page, click System Properties.
2. In the Alert Hour Settings section, check each day for which you want to set specific hours.

   Note: To specify an entire non-business day, for example, on a statutory holiday, leave the appropriate day unchecked.
3. In the Start Time boxes, select the hour and minutes at which the non-business hours begin.
4. In the End Time boxes, select the hour and minutes at which the non-business hours end.

   Result: The Alert Hours last for... boxes display how many hours and minutes you have selected. You can use this to confirm that you have entered the Start and End times correctly.
5. Click Save.

Changing the traffic units

Introduction

Data from the Channel Usage Report and the System Traffic Summary Report can be shown in centa-call seconds (CCS) or Erlangs.

- **erlang**—An international unit of the average traffic intensity (occupancy) of a facility during a period of time, normally a busy hour. The number of erlangs is the ratio of the time during which a facility is occupied (collectively or cumulatively) to the time this facility is available for occupancy.
- **centa-call seconds (CCS)**—The American unit of telephone traffic.

Note: 1 Erlang = 36 CCS

To change the traffic units

1. On the CallPilot Reporter page, click System Properties.

   Result: The System Properties window appears.
2. In the Traffic Unit Settings section, do one of the following:
   - To display information in centa-call seconds, select CCS.
   - To display information in erlangs, select Erlangs.
3. Click Save.

Troubleshooting

Introduction

If you encounter problems with Reporter, there are several sources of information:

- **Windows NT Event Log**
  - Use the Event Log on the Reporter web server to identify low level errors and situations where Reporter has problems accessing the OM database.
  - Use the Event Log on the CallPilot server to identify problems with the OM server.
- **Reporter Log**
  - Use the Reporter Log to identify Reporter-specific errors.

If you report a problem with CallPilot Reporter, the Help desk representative may ask you to look at and report some information from the Reporter Log.

To view the Reporter Log

1 On the CallPilot Reporter page, click System Log.

2 To close the System Log window, click ☒.

To delete all errors from the Reporter Log

1 On the System Log page, click Clear All.

Result: A confirmation dialog box appears.

2 Click OK to confirm.

Chapter 4

Interpreting reports and alerts

In this chapter

Types of reports

Introduction

Reports are grouped into categories according to the type of information they display.

Report type	More information
System reports System reports show trends and patterns related to system usage. For example, the Service Quality Summary Report shows the number of calls processed by voice, fax, and speech-activated messaging channels.	See Chapter 5, “System status reports.”
Messaging reports Messaging reports show trends and patterns related to the messaging programs installed on your CallPilot system. For example, the Inactive User Report shows which users are not using their mailboxes. The Top Users of Storage Report shows which users are using excessive amounts of voice storage.	See Chapter 8, “Messaging reports.”
Outcalling reports Outcalling reports show trends and usage patterns related to outcalling activity. For example, the Fax Print Audit Trail Summary Report shows faxes that have failed to print. The Fax on Demand Audit Trail Detail Report shows faxes that failed to transmit.	See Chapter 10, “Outcalling reports.”

Report type	More information
Multimedia application report The multimedia application report analyzes service activity for voice menus, announcements, and fax on demand. The multimedia application report includes the Building Block Summary Report.	See Chapter 9, “Multimedia report.”
Networking reports Networking reports show trends and patterns related to networking activity.	See Chapter 4, “Interpreting reports and alerts.”
Traffic reports Traffic reports show how much the system is being used. For example, the Productivity Report shows the total number of ingoing and outgoing calls processed by the CallPilot system. The System Traffic Summary Report shows the number of times each service is accessed.	See Chapter 7, “Traffic reports.”
Bill-back reports Bill-back reports monitor how often users access services that have a fee associated with them (such as long distance). Typically, the information contained in bill-back reports is exported to an external billing program. This allows administrators to charge the appropriate user or department for service usage.	Chapter 12, “Bill-back reports.”
Administration report The Administration Action report provides information about changes performed by administrators. They also give brief explanations of actions and the items affected by these actions.	See Chapter 6, “Administration report.”

Report type	More information
Alert reports Alert reports point out possible hacker activity on your system and failures that may be caused by software problems.	See Chapter 13, “Alert reports.”

Benefits of reports and alerts

Introduction

Analyze the information in reports to help you

- establish a pattern of normal behavior
- monitor system usage
- assess your system’s overall efficiency
- detect potential system problems
- monitor system security
- bill users for service usage
- monitor administrative changes
- identify alerts from possible hacker activity
- identify alerts from potential software problems

Use reports to establish a baseline

Generate reports on a regular basis to establish a pattern of normal behavior or “baseline” for your system. This baseline lets you differentiate between normal system activities and unusual or suspicious activities. Once you have established a baseline, you can use reports to identify potential problems.

Example

Channel Usage Reports from the last three months show that each of your channels processes an average of 50 calls per hour. If one channel suddenly drops to only three or four calls per hour, this may indicate a problem with your system’s hardware or configuration.

Use reports to monitor system usage and assess system efficiency

Study your reports to help you assess the overall efficiency of your system and decide whether changes are necessary. Among other things, reports can show

- how long callers wait before their calls are handled
- how many callers abandon their calls
- how often callers access each service or feature
- how many calls are processed by each channel
- how much free disk space is available

Example

The Service Summary Report shows the type of service accessed by callers and the number of times each service was accessed. Analyze this report to give you an overall sense of which services generate the most traffic and which services generate little or no traffic.

Use reports to detect potential system problems

Analyze the information in reports to help you identify potential system problems, such as hardware failures or inadequate resources. Some potential problems that can be detected through reports are discussed in the following examples.

Example 1: Hardware failure

If the Channel Usage Report shows that channel 4 did not handle any calls during an eight-hour period, check that this channel has been configured properly. Also ensure that the component has not malfunctioned.

Example 2: Inadequate resources

If the Service Quality Summary Report indicates that callers are experiencing a lengthy wait time before they access a channel, there may not be enough channels to handle the volume of traffic. Increase the number of channels on the system if the volume of traffic is higher than was originally anticipated.

Example 3: Inefficient usage

If the Fax Deliveries Activity Report shows that callers are not accessing the fax feature, this may indicate that

- callers do not know how to use the service. If so, you must word the service's prompts more clearly.
- callers are not aware that the service exists. Look for ways to promote the service to potential callers.
- technical problems are occurring. Investigate further and have the problems repaired.

Use reports to monitor system security

If you are concerned about the security of your system, reports can help you to detect potential hacker activity.

Example

If the Voice Messaging Activity Report indicates a discrepancy between the number of call answer sessions and the number of generated messages, this may indicate hacker activity. If hackers thru-dial out of your system during a call answer session, sessions are recorded in your report but no messages are recorded.

You can also use the Alert reports to monitor system security.

Use reports to bill service usage

Reports can also help to simplify your billing process. Bill-back reports monitor how often users access services that have a fee associated with them (for example, long distance).

Example

The DTT Usage Report tracks calls made by the DTT service to external numbers. This report records information such as

- the name and department of the user who placed the call
- the date and time of the call
- the number to which the call was placed
- the duration of the call

If some of the calls listed in this report were placed to long-distance numbers, you can determine which user or department to bill.

Use reports to track changes made by administrators

The Administration Action Report tracks changes made by administrators. This information is important because it provides a history of changes, such as when changes were made, where they were made, and who made the changes.

Use alert reports to identify alerts from possible hacker activity

Alert reports point out excessive attempts to log on to your system, indicating possible interference by hackers.

Example

The Excessive Thru-Dialer Access Alert is triggered by an unusually high number of thru-dialer accesses. This can occur if a hacker has penetrated your system and is using a thru-dialer to make toll calls.

Use alert reports to identify alerts from potential software problems

Alert reports can point out problems such as failed fax delivery or failed RN sessions that may be caused by software problems.

Example

When the Failed DTT Alert report shows an unusually high number of Delivery-to-Telephone messages are not received, it may indicate a problem with the DTT service setup.

Guidelines for interpreting reports and alerts

When you interpret reports, consider the following guidelines:

- **Determine your system size**—Know your system's disk capacity and the number of channels that are installed. Use this information to identify when you are reaching resource limits and to plan for future upgrades.
- **Establish a baseline**—Learn what is normal or average behavior for your system. Establish a baseline to help you differentiate between normal system activities and unusual or suspicious activities.
- **Consider external factors**—If your reports show unusual system activities, consider external events. For example, an extremely low volume of traffic for a Monday afternoon can be the result of a national holiday.
- **Observe day-to-day system use**—Learn how your organization operates on a day-to-day basis. The information contained in reports often relates directly to your company's routines and schedules. For example, if a large number of employees are working overtime, your reports may indicate a high percentage of after-hours logons. If you do not know how the organization functions, find someone who can help to interpret your report.
- **Consult users**—Consult the users of the system for further insight into your reports. Find out if the system is working for the users and if they have any problems to report. Some system problems result from improper use of the system (perhaps due to a lack of end-user training).
- **Consider new features or services**—Consider how long a feature or service has been in operation. If users are curious about a new feature, it may generate more traffic than usual. If users are not familiar with the feature, it may generate less traffic.

Reports and changes to server time

Changes to the server time affect the accuracy of reports. When a report is generated that includes a date on which the server time was changed, the data generated for that time can be inaccurate.

The server time can change for various reasons:

- daylight saving time
- server battery change
- server resynchronized with switch time

If the server time has been advanced by one hour, the generated data of calls made during that time shows time lengths increased by one hour. Totals and averages of call sessions displayed in reports covering the time change are also increased.

Example 1

Server time is advanced by one hour due to daylight saving time. Calls in progress when the time was changed are increased by one hour.

Actual call length: 5 minutes
Report data shows: 1 hour 5 minutes

If the server time has been decreased by one hour, the generated data of calls made during that time can show negative time lengths. Totals and averages of call sessions displayed in reports covering the time change are also decreased.

Example 2

Server time is decreased by one hour due to daylight saving time. Calls in progress when the time was changed are decreased by one hour.

Actual call length: 5 minutes
Report data shows: -55 minutes

Chapter 5

System status reports

In this chapter

Service Quality Summary Report

How to use this report

This report summarizes the level of activity for each type of channel installed on your system. Use this report to assess the service level each channel type provides to callers to the system.

The report allows you to determine whether there are adequate channel resources or whether the minimum/maximum channel settings in the SDN table need adjustment to provide the quality of service needed for callers to the system.

Use this report to determine

- how many callers are forced to wait before accessing a channel
- how many callers abandon their calls

Additional information

This report is available only to CallPilot systems that are connected to the M1 switch.

Report data

Date	The date of the reporting period.
Time Period	The time of the reporting period.
All Channels Busy (mm:ss)	The length of time in minutes and seconds that all the channels on your system were busy.
Voice Waited	The number of callers who waited for a voice channel.

Voice Abandoned	The number of callers who abandoned their calls while waiting for a voice channel.
Fax Waited	The number of callers who waited for a fax channel.
Fax Abandoned	The number of callers who abandoned their calls while waiting for a fax channel.
SR Waited	The number of callers who waited for a speech recognition channel.
SR Abandoned	The number of callers who abandoned their calls while waiting for a speech recognition channel.

How many callers waited for a channel?

Check the number of callers who waited for a voice, fax, or speech recognition channel.

If the voice, fax, or SR waited field = 0 for all time periods during a business day, then the system is providing perfect service and, therefore, has adequate resources for that type of channel.

If callers are waiting, then the service levels are less than perfect. To raise service levels requires either additional channel resources or reallocation of system resources.

Suggested actions

- Check the SDN Table to see if one of the services has a minimum channel setting that might be unnecessarily tying up channels and preventing callers to other services from getting a channel without waiting. Reduce the minimum channels guaranteed for one service to improve service quality to callers to other services.

- Check the SDN Table to see if one or more of the services have a maximum channel setting that prevents callers to the service from getting a channel without waiting. Increase the maximum to reduce the chance of callers waiting for a channel to get to the service.
- The number of voice, fax, and SR traffic channels might be out of balance with the busy hour voice, fax, and SR traffic. For example, if fax channels are under-utilized but callers to speech recognition channels have to wait, you might consider reallocating some fax resources to SR. This requires a new keycode and possibly additional channel capacity. Contact your distributor.
- Run the Service Quality Detail Report for more information about how long callers waited before accessing a channel. Refer to “Service Quality Detail Report” on page 97.

How many callers abandoned calls?

Check the number of callers who abandoned a voice, fax, or speech recognition channel. If a large number of callers abandon their calls, they might be frustrated with long wait times.

Suggested actions

- Implement one of the following options:
  - Increase the number of channels on the system (contact your distributor).
  - Use the SDN Table to reallocate existing channels. For example, if a large number of callers are waiting to access voice channels, you can configure more channels for voice.
- Run the Channel Usage Report to view the state of each individual channel. Refer to “Channel Usage Report” on page 100.

Service Quality Detail Report

How to use this report

This report provides detailed information about the grade of service provided by each type of channel. These details can help you to improve the efficiency with which callers access your services. Use this report to

- follow up on results from the Service Quality Summary Report
- determine how long callers waited before accessing a voice, fax, or speech recognition channel
- determine how many callers abandoned their calls to a specific type of media

Additional information

This report is available only to CallPilot systems that are connected to the M1 switch.

Report data

Date	The date of the reporting period.
Time Period	The time of the reporting period.
Media Type	The media type of the channels reported. They are voice, fax, or SR. The numeric values are 1= voice, 2 = fax, 3 = SR.
Number of Callers Waited	The number of callers who waited.
Percentage Calls Waited	The percentage of calls that waited.

Average Wait Time (mm:ss)	The average time a caller waited.
Maximum Wait Time (mm:ss)	The maximum time a caller waited.
Number of Callers Abandoned	The number of callers who abandoned their calls while waiting.

How long did callers wait before accessing a channel?

Check the average wait time for each type of media. If callers wait a long time before they access a resource, they might become frustrated and abandon their calls.

Suggested actions

- Check the SDN Table to see if one of the services have a minimum channel setting that might be unnecessarily tying up channels and preventing callers to other services from getting a channel without waiting. Reduce the minimum channels guaranteed for one service to improve service quality to callers to other services.
- Check the SDN Table to see if any services have a maximum channel setting preventing callers to the service from getting a channel without waiting. Increase the maximum to reduce the chance of callers waiting for a channel to get to the service.
- The number of voice, fax, and SR traffic channels might be out of balance with the busy hour voice, fax, and SR traffic. For example, if fax channels are under-utilized but callers to speech recognition channels have to wait, consider reallocating some fax resources to SR. This requires a new keycode and possibly additional channel capacity. Contact your distributor.

How many callers abandoned calls to a specific type of media?

Check the media type and the number of abandoned calls. If many callers abandon their calls to a particular media type, you might not have enough channels configured for that media type. For example, if callers abandon calls to fax channels because of lengthy wait times, you can configure additional channels to handle fax.

Suggested actions

- If callers are abandoning their calls to a specific media type because of frustration over long wait times, consider increasing the number of channels that handle the type of media.
- Run the Channel Usage Report to view the state of each channel. This ensures that your channels are operating correctly. Refer to “Channel Usage Report” on page 100.

Channel Usage Report

How to use this report

This report summarizes the traffic handled by each channel on your system. Use this report to identify

- traffic distribution patterns
- problems with specific channels
- short call durations

Additional information

You can print this report as a graph.

Report data

Date	The date of the reporting interval.
Time Period	The time of the reporting interval.
Channel Number	The number of the multimedia channel.
Incoming Calls	The number of incoming calls on each channel.
Outgoing Calls	The number of outgoing calls on each channel.
Total Calls	The total number of incoming and outgoing calls on each channel.
Avg. Hold Time Incoming Calls	The average hold time in seconds of incoming calls on each channel.
Avg. Hold Time Outgoing Calls	The average hold time in seconds of outgoing calls on the channel.

CCS/Erlang	**CCS:** The amount of traffic, in centa-call seconds (CCS), that the channel handled per hour, during the period (the numbers are rounded to the nearest integer, with the total being the total of the rounded integers.) A single channel can handle a maximum of 36 CCS. **Erlangs:** The number of Erlangs are rounded to two decimals, with the total being the total of the rounded numbers. A single channel can handle a maximum of 1 Erlang. **Note:** Information is shown in either CCS or Erlangs. For more information see, “Changing the traffic units” on page 80.

Is traffic evenly distributed across your channels?

Compare the number of ingoing and outgoing calls for each channel. The average amount of traffic for each channel should be similar. If a channel shows no incoming or outgoing calls, the channel might be disabled or faulty.

Suggested actions

Use the Multimedia Channels program and the DS0 Channels program to check the channel’s state.

- If the channel is disabled, use the Maintenance program to enable the channel.
- If the channel is faulty, use the Maintenance program to run diagnostics on the channel.

Is Average Hold Time unusually short?

Compare the number of incoming calls with the length of each call. Channels with a high number of incoming calls but low CCS times mean that calls are very short. Channels with unusually short Average Hold Time (AHT) might indicate a problem with that channel.

Suggested action

Run the traffic reports to obtain more information about the problem. Refer to Chapter 7, “Traffic reports.”

Multimedia File System Usage Monitor Report

How to use this report

Use this report to determine whether the system has sufficient disk volume storage to handle the current messaging and multimedia applications.

If a multimedia File System Volume becomes full, users with mailboxes on that volume cannot create or receive any new messages. Therefore, it is very important that a volume is not allowed to fill up.

A major alarm is raised when a volume capacity reaches 90%. A critical alarm is raised when a volume capacity reaches 95%.

Additional information

You can print this report as a graph.

Report data

Date	The date of the information.
Time	The time of the information.
Volume ID	The ID of the storage volume. Volumes are sections on the Nortel Networks disk.
Voice Capacity (hh:mm)	The amount of voice storage space available in hours and minutes.
Voice Used (hh:mm)	The amount of voice storage space used in hours and minutes.

Percentage of Text Used	The percentage of text capacity that is currently in use.
Percentage of Voice Used	The percentage of voice capacity that is currently in use.
Text Capacity (kbytes)	The amount of text space currently available, in kbytes.
Text Used (kbytes)	The amount of text space currently used, in kbytes.

Is your capacity over 90 percent?

Suggested actions

- Check the time on the report. Storage usage often fluctuates during the day. For example, storage generally peaks right before the start of the working day when users are not available to receive voice or text messages.
- Storage usage also varies over the course of a week. Read messages are deleted automatically each night. On Friday, storage usage is high but by Monday, storage usage is low as there are no new read messages over the weekend.
- Run the Top Users of Storage Report to identify mailboxes that are storing too many messages (refer to “Top Users of Storage Report” on page 144). You can reduce the message retention time, reduce message length parameters, or move mailboxes with high-usage volumes to low-usage volumes. Only technical support personnel and Distributors can move users from one volume to another.
- Increase the storage capacity of the system. Contact your distributor.
- Check the Alarm Monitor to see if there are any events indicating problems with the MMFS and its nightly audit. There might be a problem that is preventing the space held by deleted messages from being recovered. If these events exist, contact your distributor immediately.

Disk Usage Report

How to use this report

Use this report to determine whether the system has sufficient disk drive storage. The first disk drive holds

- the Operating System
- the CallPilot software
- the CallPilot database
- the first Multimedia volume VS1

The size of your Multimedia volume depends on the number of hours that are purchased.

A larger CallPilot system might have additional disk drives containing additional Multimedia volumes (VS102, VS103). The size of these addtional volumes depends on the number of hours that are purchased.

Additional information

You can print this report as a graph.

Report data

Date	The date of the information.
Time Period	The time period of the information.
Disk Capacity (kbytes)	The amount of disk space currently available, in kbytes.
Disk Used (kbytes)	The amount of disk space used, in kbytes.

Percentage Disk Used	The percentage of disk space used.
Disk Drive	The disk drive used.

Check available disk space

Compare the disk capacity to the percentage of disk space used.

Suggested actions

If the report indicates that the disk drive is full, call your Distributor.

Note: The CallPilot system continues to operate; however, future upgrades might be affected.

Chapter 6

Administration report

In this chapter

Administration Action report

How to use this report

Use this report to obtain high-level information on changes made to the CallPilot system by administrators. This information can be useful if you need to determine

- whether changes have recently been made to CallPilot
- which administrator made those changes
- the client from which those changes were made

Additional information

The actions for this report are grouped under the Create, Delete, and Modify subgroups.

The Administration Action report is the default report for the Administration category. A copy of this report is generated automatically when a new system is created. Existing systems generate this report by running the New Reports utility of the Reporter Application.

Report data

Date	The date when the action was generated.
Time	The time when the action was generated.
Administrator Name	The full name of the administrator responsible for executing the changes.
Action Type	This can be Create, Modify, or Delete.
Client Network Address	The network IP address for the client from which the changes were made.

Object	The item or items that are affected from this action. They are as follows: - Users - Mailbox Class - SDL - Message Delivery - Messaging Administration - Outcalling Administration - Security Administration - RPL - Messaging Network - Internet Mail - System Prompt - Application Builder - Service DN
Description	A high-level description of the changes.

Limitations

The Administration Action report does not provide specific information about modified items. The collected data only indicates that a modification has occured.

The Affected Item filtering criteria filters all actions according to a specific item. As the content of this item varies greatly, use another filtering item to create proper filtering criteria.

You cannot print this report as a graph.

Chapter 7

Traffic reports

In this chapter

Productivity Report

How to use this report

Use this report to obtain information on productivity gains from using the CallPilot system. This information can be useful if you need to demonstrate

- the quantity of service provided by CallPilot
- the cost effectiveness of CallPilot
- an economic justification for CallPilot services

Report data

Calls Summary	
Number of Incoming Calls	The number of calls that came in to the CallPilot system.
Number of Outgoing Calls	The number of outgoing calls originated by the CallPilot system.
Total Calls	The total number of incoming and outgoing calls to the CallPilot system.
Total Connect Time (Hours)	The total amount of connect time, in hours, due to all calls to and from the CallPilot system.
Equivalent Person Weeks	The number of 40-hour person-weeks required to handle the same service that CallPilot provided during the specified date/time interval.
Messaging Sessions	
Number of Express Voice Messaging Sessions	The total number of express voice messaging sessions.

Number of Call Answering Sessions	The total number of call answering sessions.
Number of Express Fax Messaging Sessions	The total number of express fax messaging sessions.
Number of Fax Call Answering Sessions	The total number of fax call answering sessions.
Number of Logon Sessions	The total number of logon sessions.
Number of Speech-Activated Messaging Sessions	The total number of speech-activated messaging sessions.
Messages Created	
Number of EVM/CA Voice Messages	The total number of voice messages created by Express Voice Messaging and Call Answering.
Number of EFM/FCA Fax Messages	The total number of fax messages created by Express Fax Messaging and Fax Call Answering.
Number of Logon Voice Messages	The total number of voice messages created during any type of session, including DTMF log on, voice/fax log on, or speech activated messaging.
Number of Logon Fax Messages	The total number of fax messages created during any type of session, including DTMF logon, voice/fax log on, or speech activated messaging.
Other Activity	
Application Builder	The total number of Application Builder sessions.
Remote Notification	The total number of remote notification attempts.
Delivery to Telephone	The total number of delivery to telephone attempts.
Fax Deliveries	The total number of fax delivery attempts.

Enterprise Networking	The total number of Enterprise Networking calls.
AMIS Networking	The total number of AMIS Networking sessions. This includes Integrated and Open AMIS.

System Traffic Summary Report

How to use this report

This report summarizes information about traffic patterns in your CallPilot system. Use this report to identify

- busy hours for your system
- services that are not being used
- services that are generating an unusually high amount of traffic
- periods when users have trouble logging on
- users who are not responding to their voice mail

Additional information

You can print this report as a graph.

Report data

Date	The date of the report.
Time Period	The time period of the report.
Service Name	The name of the service, such as call answering, that was accessed.
Total Accesses	The total number of accesses made to the service.
Average Hold time (mm:ss)	The average length, in minutes and seconds, of an access to the service during the specified period.

CCS/Erlang	The traffic in centa call-seconds (CCS) or Erlangs. The numbers in a CCS calculation are rounded to the nearest integer, with the total being the total of the rounded integers. The numbers in an Erlang calculation are rounded to two decimals, with the total being the total of the rounded numbers.
Percentage of Period Total	The percentage of total traffic that this service generates.

Identify busy hours for your system

Run this report with the interval set for one day, midnight to midnight. A bar graph is generated showing the traffic and accesses for each hour of the day. From this graph, it is possible to observe peak hours for traffic.

Note: If the reporting interval is 24 hours a day or less, the graph displays a bar of data for each hour. Otherwise, the graph shows a bar of data for each day.

Suggested action

Run the service quality summary report to see if there are callers waiting or abandoning during the busy hour. If they are, then the System Traffic Summary Report tells what services they are trying to reach and can aid in identifying which services should have minimum and maximum channels adjusted in the SDN Table (see “System Traffic Summary Report” on page 115).

Identify services that are not being used

Check the number of accesses for each service. If a service has a low number of accesses, the service might not be working properly, or users might not be aware that it exists.

Suggested actions

- Ensure that the service has been installed on your CallPilot system.
- Ensure that the service is working correctly.
- Ensure that users are aware of the service and have been properly trained to use it.
- Check the time of the reporting interval. In some organizations, it is normal for certain services to be used less during some periods than others.

Identify services that are generating an unusually high amount of traffic

Check the Total Accesses field. If the number of accesses is higher for this service than for other services listed in the report, you might experience system performance problems.

Suggested actions

- Check that the high volume of traffic was not caused by an unusual event. For example, if you work for an airline company that advertises a one-day discount, expect unusually high usage statistics from a particular feature.
- If the high traffic for a particular service is expected to continue, you can set a minimum number of channels that must be available to a service in the SDN table. You can also expand the system if the overall traffic is higher than originally anticipated.
- If the problem is that a particular service is experiencing sporadic traffic spikes, and it is a less important application than others (like call answering), then consider setting a maximum number of channels for this service in the SDN Table.

Identify periods when users are having trouble logging on

If users are having trouble logging on to CallPilot at certain times, check the level of traffic for that time period.

Suggested action

- Check to see if periods when users cannot log on coincide with peak traffic hours for your system. If so, consider adding resources or reallocating them to better serve callers.
- Check the SDN Table for services with non-zero minimum channels settings and consider lowering the minimums.

Identify users who are not responding to their voice mail

Compare the number of accesses with the logon count provided by the Voice Messaging Activity Report (see “Voice Messaging Activity Report” on page 131). If the logon count is low compared to the number of accesses, users are accumulating several messages before logging on to listen to them. Too many accumulated messages lowers the amount of available disk space to the point where overall system performance can be affected.

Suggested actions

- Encourage users to keep up to date with their voice mail and faxes.
- Reduce the maximum allowable message length or increase storage capacity of the system. Contact your distributor.
- Run the Call Answering/User Responsiveness report to identify users who are not responsive (see “Call Answering/User Responsiveness Report” on page 120).

Chapter 8

Messaging reports

In this chapter

Call Answering/User Responsiveness Report

How to use this report

This report shows information about Call Answering (CA) and Express Voice Messaging (EVM) on a per-user basis. Use this report to identify users who are not

- receiving voice messages
- logging on to their mailbox

Report data

Name	The name of the mailbox owner.
Mailbox	The mailbox number.
Date	The date of the report interval.
Total CA+EVM Calls	The total number of Call Answering and Express Voice Messaging calls.
No Msg CA+EVM Calls	The total number of calls that resulted in no message being left by the caller. A no-message call occurs when a caller is routed to Call Answering for a mailbox and does not leave a message.
Percentage Of No Message Calls	The percentage of no message calls to total calls.
Logons	The number of successful logons.
CA+EVM Message Received	The total number of Call Answering and Express Voice Messages with message being left by the caller.

Logons per Message	The percentage of number of successful logons to Call Answering and Express Voice Messages with message being left by the caller.

Identify users who are not receiving messages

Compare the total number of no-message calls with the total number of CA and EVM calls. If there is a higher percentage of calls than messages, users are hanging up without leaving a message, or are pressing 0 to speak to an attendant.

Suggested actions

- Ask users to review their greetings. If greetings are unfriendly or instructions are too complex, callers might hang up without leaving a message.
- Listen to the users’ greetings.
  - If a greeting indicates an extended absence, expect a high percentage of no-message calls.
  - If users have not recorded a greeting, ask them to record one as soon as possible. If users are not available, record a temporary greeting on their behalf.
- Provide users with additional training on how to compose and maintain greetings.

Identify users who are not logging on to their mailbox

Compare the total number of CA and EVM calls to the number of logons. If there are more messages than logons, users are not retrieving their voice messages.

Suggested actions

- Find out if a user is absent. If so, you can archive the user’s messages to tape.
- Check the user’s greeting. If the user is absent but has not indicated this in his or her greeting, you can record a temporary absence greeting on his or her behalf.

Inactive User Report

How to use this report

This report shows users who are not maintaining their mailboxes. Use this report to identify users who are not

- logging on to their mailboxes
- reading their messages

Report data

Name	The user name associated with the mailbox. The report shows only the users whose last logon session preceded the Last Logon date.
Mailbox	The mailbox number of the user.
Unread Messages	The number of messages that were left unread at the time of the last logon session. If this field is blank, the user has not logged on during the range of dates in the database.
Last Log on date	The date of the last logon.
Last Log on Time	The time of the last logon. If this field is blank, the user has not logged on during the range of dates in the database.

Identify users who are not logging on to their mailboxes

Check the user name and the last logon date. If users are not logging on to their mailboxes regularly, your messaging system is not being used effectively.

Suggested actions

- Check to see if any users are on vacation or extended leave.
- Remind users that stored messages consume disk space.
- When users leave the company, ensure that their mailboxes are removed from distribution lists. Unused mailboxes that are included on distribution lists continue to store messages that are sent to their owners.
- Use the Mailbox Call Session Summary Report to follow up on lack of user responsiveness (see “Mailbox Call Session Summary Report” on page 125).

Identify users who are not reading their messages

Check the user name and the number of unread messages. If users store messages over a long period of time, a high percentage of disk space is used. This can result in poor system performance.

Suggested actions

- Remind users that stored messages consume disk space.
- Provide additional training for users.
- Use the Mailbox Call Session Summary Report to follow up on lack of user responsiveness (see “Mailbox Call Session Summary Report” on page 125).

Mailbox Call Session Summary Report

How to use this report

This report provides information about each call session to a particular mailbox during the reporting period. Use this report to

- follow up on lack of user responsiveness
- identify suspicious caller DNs and long sessions that might indicate hacker activity
- investigate user complaints of delayed messages

Report data

This report lists each call made to a mailbox during the reporting period and provides the following details:

Header: User Name, Mailbox Number	Indicates the user’s name and the mailbox number.
Date/Time	The date and time of the call.
Session Length	The length of the session in hours, minutes, and seconds (hh:mm:ss).
Session Type	The type of session: VM—Voice Messaging MM—Multimedia Messaging EVM—Express Voice Messaging SAM—Speech Activated Messaging CA—Call Answering

Session Type (continued)	FCA—Fax Call Answering EFM—Express Fax Messaging This field includes the count of invalid logon attempts.
Caller DN	The telephone number (either internal extension or external phone number) that originated the call to the mailbox. This field can contain up to 17 digits.
CA/EVM Voice Msg Received	The total number of voice messages left during the CA or EVM session.
FCA/EFM Fax Msg Received	The total number of fax messages that arrived during the FCA or EFM session.
Msg Read	The total number of voice and fax messages that were read during the logon session.
Msg Sent	The number of voice and fax messages that the user sent during the logon session.
Msg Unread	The total number of unread voice and fax messages at the end of the session.
Session End Indicator	Shows how the session ended: ▪ applications error ▪ hung up ▪ time-out ▪ log off ▪ log on ▪ transfer ▪ switched to fax mode ▪ unknown
Transfer DN	If there was a call transfer during the session, this is the DN to which the caller was transferred.

Identify sources of low user responsiveness

Identify sources of low user responsiveness by looking at the following fields:

- Add the values in the CA+EVM Msg Received and FCA/EFM Fax Msg Received fields. Compare this total to the value in the Msg Read field. If the number of read messages is lower than the total of the messages received, the user is not listening to all of his or her messages.
- Check the Session Type field to find users who do not log on often (few VM, MM, or SAM sessions).
- Check the Msg Unread field for unread messages at the end of a session.

Suggested actions

- If users are not logging on to their mailboxes or listening to messages, see if they need additional training.
- If a user is reporting delayed messages, check to see if unread messages (Msg Unread field) exist at the end of the logon sessions. If they do, the user might think the messages were not delivered until the next logon time. Some users might need training on how to retrieve messages.

Identify suspicious caller DNs

If you suspect that a hacker is trying to access or has gained access to a particular mailbox, look at the sessions for that mailbox and identify the caller DNs. One of the DNs calling in to the mailbox could belong to the hacker.

Suggested actions

Enable Hacker Monitor to track suspicious caller DNs (referred to as CLIDs in Hacker Monitor). Whenever a monitored DN calls in to the system and logs on to a mailbox or places a thru-dial call, an alarm is generated in real time to notify you.

Identify long sessions

Check the Session Length field for especially long sessions (particularly CA and logon sessions). These indicate that a hacker has accessed the mailbox and has found a way to dial out from your system to place long distance calls. Once in a mailbox, the hacker can set up a session and leave it open for a long time to sell services.

Suggested actions

- Check the status of the mailbox and its owner. Is the user actively using the mailbox, on vacation or extended leave, or no longer with your company?
- If the mailbox is unused because the user is no longer with your company, delete the mailbox immediately. Unused mailboxes are the targets of hackers and must be removed.
- If the user is temporarily away, you can either change the user’s password or disable the mailbox until the user returns.
- If the mailbox is active, inform the user of the situation and ask the user to change the password immediately. Give the user tips on how to create secure passwords.
- Monitor the mailbox regularly.

Identify short sessions ending with a transfer

Look for mailboxes with a number of short logon sessions ending with a transfer. This is strong evidence that someone is using the mailbox just to place calls.

Suggested actions

- Check if the mailbox is used by a current employee.
- Check if the greeting suggests that the employee is not checking his or her mailbox.
- Check the restriction/permission list of the Mailbox Class to which the mailbox belongs.
- Force a password change to block further access.
- Enter the Caller DN of repeat callers into the hacker monitor.

Mailbox Counts Report

How to use this report

This report counts the number of mailboxes by mailbox class, department, and switch location. Use this report to get statistical information about the number of mailboxes in each department or switch location.

Report data

Mailbox Counts (Mailbox Class) Report	
Mailbox Class	The name of the mailbox class.
Mailbox Count	The total number of mailboxes.
Mailbox Counts (Department) Report	
Department	The department name.
Mailbox count	The total number of mailboxes.
Mailbox Counts (Switch Location) Report	
Switch Location	The name of the switch location.
Mailbox Count	The total number of mailboxes.

Voice Messaging Activity Report

How to use this report

This report summarizes the voice messaging activity on your CallPilot system. Use this report to

- identify a high number of calls and long messages
- identify high numbers of abandoned calls
- identify discrepancies between the number of sessions and the number of messages
- gain an understanding of the number and length of each type of messaging session

Report data

Date	The date of the reporting interval.
Time Period	The time of the reporting interval.
CA/EVM Sessions	The number of Call Answering and Express Voice Messaging sessions during the specified time period.
Logon Sessions	The number of voice messaging logon sessions during the specified time period.
Speech Rec. Messaging Sessions	The number of Speech Rec. Messaging sessions during the specified time period.
Desktop Message Transfer	The number of new voice messages received by clients.
Average Session Length (sec.)	The average length in seconds of CA, EVM, and logon sessions for the specified time period.

Maximum Session Length (sec.)	The longest length in seconds of CA, EVM, and logon sessions for the specified time period.
Call Answering Messages Created	The number of CA messages created during the specified time period.
Logon Messages Created	The number of logon messages created during the specified time period.
Average Message Length (sec.)	The average length of messages, in seconds, created during the specified time period. Since message length affects disk storage, use this information to determine whether enough disk space has been allocated for voice messages.
Maximum Message Length (sec.)	The longest message created during the specified time period.

Identify a high number of calls and long messages

Compare the number of calls with the average message length. Too many calls in a short period of time, combined with users leaving long messages, ties up channels and prevents others from accessing the CallPilot system.

Suggested actions

- Reduce the maximum allowable length for messages.
- Consider expanding your system.

Identify a high number of abandoned calls

Compare the number of CA or EVM messages to the total number of CA or EVM sessions. If there are fewer messages than sessions, callers are abandoning their calls.

Suggested actions

- Ask users to review their greetings. If greetings are unfriendly or instructions are too complex, users might hang up without leaving a message.
- Listen to users' greetings.
    - If a greeting indicates an extended absence, expect a high percentage of no-message calls.
    - If users have not recorded a greeting, ask them to record one as soon as possible. If the users are not available, record a temporary greeting on their behalf.
- Provide users with additional training on how to compose and maintain greetings.

Identify discrepancies between the number of sessions and the number of messages

Compare the total number of CA sessions with the total number of CA messages created. The number of sessions should match or be similar to the number of messages created. If there are more sessions than messages, this means that after reaching the CA greeting, users are hanging up without leaving a message, or they are pressing 0 to transfer to an attendant. Callers might hang up without leaving a message if they are not familiar with the service. If hackers thru-dial out of your system during a CA session, you will receive CA sessions but no messages.

Suggested actions

- Users might need some training on using CA and EVM.
- Users should review their greetings. If greetings are unfriendly or instructions are too complex, callers might hang up without leaving a message.
- Run the Call Answering/User Responsiveness Report to determine which mailboxes have a high percentage of no-message calls (see “Call Answering/User Responsiveness Report” on page 120).
- If you suspect hacker activity, check the restriction/permission list that is assigned to the Call Answering/Express Voice Messaging Thru-Dial feature. You can also examine the Excessive Incomplete Messaging Accesses Alert (see “Excessive Incomplete Messaging Accesses Alert” on page 226).

Desktop Messaging Activity Report

How to use this report

This report summarizes the activity for the Desktop Messaging program on your CallPilot system. Use this report to determine how many

- voice messages are received by clients
- fax messages are received by clients

Report data

Date	The date that the activity took place.
Time Period	The start and end time between which the activity took place.
New Voice Presented	The number of new voice messages received by clients.
New Fax Presented	The number of new fax messages received by clients.

Identify number of fax messages received by clients

Check the New Fax Presented field.

Identify number of voice messages received by clients

Check the New Voice Presented field.

Fax Messaging Activity Report

How to use this report

Use this report to summarize the fax messaging activity on your CallPilot system. This report gathers fax usage statistics for individual mailbox users.

Report data

Date	The date of the reporting period.
Time Period	The time of the reporting period.
Fax Call Answering Sessions	The number of times callers were routed to Fax Call Answering on the CallPilot system.
Express Fax Messaging Session	The number of times callers dialed the Express Fax service, which allows them to leave a fax message in a specific mailbox.
Call Answering Faxes Created	The number of fax messages created after callers were routed to the CallPilot system.
Express Faxes Created	The number of fax messages created after callers dialed the Express Fax service.
Logon Faxes Created	The number of fax messages created by users logged on to the CallPilot system.
Average Fax Size (pages)	The average number of pages that make up one fax message.
Fax Print Sessions	The number of fax messages printed by users logged on to the CallPilot system.
Desktop Message Transfers	The number of new fax messages received by clients.

How much fax traffic does each mailbox user handle?

Check the following fields to obtain information about the volume of fax traffic handled by each user:

- Call Answering Faxes Created
- Auto Attendant Faxes Created
- Average Fax Size (pages)
- Desktop Message Transfers

Suggested action

Assign users who handle a high volume of faxes to a mailbox class with more storage capacity.

Are callers leaving fax messages?

Compare the number in the Fax Call Answering Sessions field with the number in the Call Answering Faxes Created field. Compare the number in the Fax Auto Attendant Sessions field with the number in the Auto Attendant Faxes Created field. If the number of sessions is much greater than the number of faxes created, then callers might not understand how to leave a fax message, or a nonexistent mailbox might be specified for Fax Auto Attendant.

Suggested actions

- Review the prompts used for Fax Call Answering to determine if they can be made more direct and helpful. If so, rerecord the prompts.
- If only one mailbox is specified for Fax Auto Attendant, make sure the mailbox number is correct.

Messaging Usage Report

How to use this report

This report provides a daily summary of how many system resources a mailbox is using. It reports on the amount of channel, storage, and network resources used, as well as the aggregate number of messages sent and received. Use this report to gather statistics for a mailbox's

- resource usage
- messages sent and received

Additional information

When running or printing this report, specify a period of at least 24 hours of data be included in the report. This ensures that the information spans a significant length of time.

Report data

Name	The first and last name of the mailbox owner.
Mailbox	The number of the mailbox.
Date	The date for which mailbox usage data is provided.
Channel Connect Time (sec)	The total amount of time that the mailbox was connected to a channel on the specified date. **Note:** The channel connect time does not include outcalling time.
Storage (mm:ss)	The average amount of disk space used by the mailbox on the specified day, in minutes and seconds. This includes the amount of space taken up by voice messages, fax messages, and greetings.

Storage (kbytes)	The average amount of disk space used by the mailbox on the specified day, in kbytes.
# of SAM Sessions	The number of Speech-Activated Messaging sessions that occurred on the specified date.
Desktop Message Transfers	The number of new voice and fax messages received by clients.
Messages Received	The total number of messages received by the mailbox on the specified date.
Messages Sent	The total number of messages originating from the mailbox on the specified date.
Total	The average amount of disk space used per mailbox on the specified date.
Grand Total	The average amount of storage space used per mailbox during the reporting interval.

How much messaging traffic does each mailbox user handle?

Check the following fields to obtain information about the volume of messaging traffic handled by each user:

- Messages Sent
- Messages Received
- Storage (kbytes)
- Number of SAM sessions

Suggested action

Assign users who handle a high volume of messages to a mailbox class with more storage capacity.

Are there long channel connect times?

Check the Channel Connect Time (sec) field for lengthy connections. These might indicate that hackers are using the mailbox to place outcalls.

Suggested actions

- Check the status of the mailbox and its owner. Try to determine if there is a reason for the lengthy connections. Is the user actively using the mailbox, on vacation or extended leave, or no longer with your company?
- If the mailbox is unused because the user is no longer with your organization, delete the mailbox immediately. Unused mailboxes are targets for hackers and must be removed.
- If the user is temporarily away, you can either change the user’s password or disable the mailbox until the user returns.
- If the mailbox is active, inform the user of the situation and ask the user to change the password immediately. Give the user tips on how to create secure passwords.
- Monitor the mailbox regularly.

Speech-Activated Messaging Report

How to use this report

This report summarizes information about each Speech-Activated Messaging (SAM) session to a particular mailbox. Use this report to gather SAM usage statistics for individual users who have reported trouble with SAM.

Report data

Header: User Name, Mailbox number	The last name and first name of the mailbox user, and the number of the mailbox.
Date	The date of the session.
Time	The time of the session.
Session Length	The length of the session.
Caller DN	The directory number from which the call originated.
Total Unsuccessful Logon Attempts	The total number of unsuccessful Speech Recognition (SR), Dual-tone multifrequency (DMTF), and Mixed logon attempts during the attempted SAM session.
Unsuccessful SAM Logon Attempts	The number of unsuccessful logon attempts to SAM using SR.
Unsuccessful DTMF Logon Attempts	The number of unsuccessful logon attempts to SAM using DTMF.
Unsuccessful Mixed Logon Attempts	The number of unsuccessful logon attempts to SAM using either SR or DTMF.

Logon Result	0 = success with SR 1 = success with DTMF 2 = success with SR and DTMF 3 = max. invalid 4 = hung up 5 = canceled 6 = timed out 7 = locked out
Total Recognitions	The total number of attempted recognitions of user speech by the speech recognizer.
Accepted Recognitions%	The percentage of attempted recognitions by SR that were successful and did not require a confirmation query of the user. These occurred because the speech recognizer was statistically confident it understood what the user said.
Queried Recognitions%	The percentage of attempted recognitions by SR that were successful but required a confirmation query of the user. These occurred because the speech recognizer thought it understood what the user said, but it was statistically unsure and queried the user to confirm.
Rejected Recognitions%	The percentage of attempted recognitions by SR that failed. These occurred because the speech recognizer did not understand what the user said and had to ask the user to try again.
DTMF Switches	The number of switches from SAM to DTMF (either 0 or 1).

High percentage of Queried or Rejected recognition attempts

A high percentage of Queried or Rejected recognition attempts indicates that the user was struggling to be recognized during this SAM session. If the user switched to DTMF, then the user “gave up” on using SR for this session.

Suggested actions

This might be a single unsuccessful SAM session for a user who normally has success with SR. There might have been temporary factors that affected SR performance, such as a bad connection or noisy background, a user not speaking normally due to fatigue, or other factors. This would be indicated if other SAM sessions for this user do not show problems.

However, some users consistently have problems with SR. Typically, users experience the greatest difficulty with having their mailbox number and password being recognized successfully. Once they are successfully logged on, they can use the SAM commands. Users who fit this profile can try some of the following alternatives:

- If the phone is not in an open office environment, program the mailbox for autologon to eliminate the need to speak the mailbox number and password.
- If users are calling from a wireless telephone, have them program the mailbox number and password into speed-dial.
- Remind users that if they are calling from a DTMF phone, they can use DTMF whenever prompted for a number, including mailbox number, password, or addresses when composing a message.
- If users are using SAM because they occasionally pick up messages from a rotary phone and do not have DTMF, then set up a SAM service that uses Paced Digit Recognition. It is slower but much more reliable at recognizing a mailbox number and passwords.

Top Users of Storage Report

How to use this report

Use this report to display the top 50 users of storage as of the date specified by the report.

Additional information

You must run the system to be reported on for at least one full day (24 hours) before the data in this report is valid.

Report data

Name	The name associated with the mailbox.
Mailbox	The number of the mailbox.
Storage Used (mm:ss)	The total storage used by the mailbox, including greetings, in minutes and seconds, taken at the date noted beneath the report title.
Storage Used (fax pages)	The total amount of disk storage used by the user, in fax pages.
Storage Used (Kbytes)	The total amount of disk storage used by the user, in kbytes.
Mailbox Class	The mailbox class for the mailbox.
Switch Location	The name of the switch location.

Which users are using the most storage?

Check the mailbox number and the total amount of disk storage taken up by each user. Storage of messages for long periods of time or storing too many messages can reduce system performance.

Suggested actions

- Remind users that stored messages take up valuable space.
- Ask users to delete old messages.
- If you suspect that users are exceeding their storage limit, run the Users Exceeding Storage Limit Report.

Users Exceeding Storage Limit Report

How to use this report

Use this report to identify users who are exceeding the storage limit established by their mailbox class.

Report data

Name	The user name associated with the mailbox.
Mailbox	The number of the mailbox.
Storage Used (mm:ss)	The total storage used by the user's mailbox, including greetings, in minutes and seconds, taken at the date noted beneath the report title.
Storage Limit (mm:ss)	The maximum storage allowed by the mailbox class.
Percent Above Limit	The storage exceeding the mailbox class, as a percentage.
Mailbox Class	The mailbox class of the mailbox.
Switch Location	The switch location of the mailbox.

Which users are exceeding their storage limit?

Check the following fields for information about users who are taking up more than their allotted percentage of disk space:

- Percent Above Limit
- Storage Used (mm:ss)
- Storage Limit (mm:ss)
- Mailbox Class

If too many users exceed their storage limit, system resources are tied up, reducing overall system performance.

Suggested actions

- Contact the appropriate users and ask them to delete old messages.
- Reduce the message retention period set in Mailbox Classes.
- Prevent mailboxes from accepting messages when they are full.
- Ask technical support to move users who need large amounts of storage to volumes on the hard disk that have more available storage space.

  Note: Administrators do not have this permission.
- Run the Call Answering/User Responsiveness Report to see if users are checking their messages (see “Call Answering/User Responsiveness Report” on page 120). If users are not checking their messages, find out if they are on extended leave. If a user is absent and his or her mailbox is exceeding capacity, you can archive his or her messages to tape.

Chapter 9

Multimedia report

In this chapter

Building Block Summary Report

How to use this report

Use this report to determine if you need to redesign any applications created with Application Builder. This report collects information about how certain building blocks are accessed by callers during a defined time period. This helps you to determine if callers are using the blocks efficiently.

Graph format

For this report, you must generate graphs on a block-by-block basis. You cannot generate one graph for the entire report. Make sure the following criteria are selected on the Selection Criteria property page:

Block Name	Is Equal To	Type the name of the appropriate block.
ServiceAppID	Is Equal To	Type the appropriate ServiceAppID.
Block Type	Is Equal To	Choose the appropriate block type: 1=Announcement 2=Thru-Dial 3=Call Transfer 4=Fax Select 5=menu

Report data

ServiceAppID	The unique number used to identify the AppBuilder application in which the block resides. If the application is in the Service DN Table, then the application is called a service.
Block Name	The name given to the block when it was placed in the application.
Block Type	The type of block. This report records information for five types of blocks: ■ Announcement ■ Call Transfer ■ Fax Select ■ Menu ■ Thru-Dial
Date	The date the report data was collected for the block.
Time	The time the report data was collected for the block.
Average Access Time	The average amount of time callers interacted with the block.
Number of Abandonments	The number of calls that were abandoned while in this block.
Number of Accesses	The number of times this block was reached/accessed.
Number of Times Each Key Has Been Used	The total number of times that callers pressed keys on the phoneset to interact with the block.
# of Faxes Selected	The number of faxes selected by callers in an application that contains Fax Select blocks.

Types of blocks

Before you can effectively use the information in this report, you must understand the difference between the types of blocks. The report information applies differently to each block.

In general, AppBuilder applications use two categories of blocks—building and system. This report is concerned with building blocks, which are combined to create voice and fax applications. System blocks are used in voice and fax applications that provide links to existing applications on the system.

In particular, this report is concerned with five types of building blocks—Announcement, Call Transfer, Fax Select, Menu, and Thru-Dial.

Announcement

The Announcement block provides the primary way to play voice in an application.

Call Transfer

The Call Transfer block transfers callers to the default attendant or an extension of their choice.

Fax Select

The Fax Select block contains a fax document that a caller can select for same-call or callback delivery.

Menu

The Menu block gives callers options and their corresponding keys on the phoneset.

Thru-Dial

The Thru-Dial block provides an automated attendant service that transfers callers to the extension of their choice.

How many times did callers press keys?

By looking at the # of Accesses field, you can determine how many times callers pressed keys for each block. A large number of key presses for a block can indicate unnecessary or misplaced information, or hacker activity.

Unnecessary or misplaced information

If the # of Accesses field contains a large number for an Announcement block, then callers are pressing keys on the phoneset to interrupt and bypass the announcement.

A large number implies one of the following situations: the announcement is unnecessary, it needs to be repositioned elsewhere in the application, or it needs to be configured so that callers cannot interrupt it.

Hacker activity

Check the # of Accesses field for the Thru-Dial block. If the field contains a large number for this block, someone might be using the application to try to place calls to long distance numbers. To discourage hacker activity, you can password-protect the Thru-Dial block. As well, you can ensure that its restriction/permission list does not allow long distance calls.

How long did callers use a block?

Look at the Average Access Time field for any block. If the average time is long, callers could be experiencing difficulty interacting with that particular block.

Consider how a block and its related voice items can hinder a caller’s interaction. For example, if callers take a long time at the Thru-Dial block, then they probably do not understand how to enter the number that they want dialed. If callers take a long time at the Menu or Fax Select blocks, they do not understand the choices associated with these blocks or how to indicate a choice.

Chapter 10

Outcalling reports

In this chapter

DTT Activity Report

How to use this report

This report monitors use of the Delivery to Telephone (DTT) service. Use this report to determine

- how much the service is being used
- if messages are being delivered
- whether the DTT service is able to acquire channels when needed
- whether the DTT retry settings are adequate

Report data

Date	The date of the specified reporting period.
Time Period	The time of the specified reporting period.
New Requests	The total number of new requests for message delivery that were made to the DTT service during the reporting period. A request is made whenever a user tries to compose and send a message to a telephone number that does not have a mailbox defined in your system.
Retry Failures	The number of times the DTT service tried to resend messages that could not be delivered because the retry limit was reached or exceeded. DTT tries to resend a message when a call attempt results in a busy, no answer, or answer (but no Dual-tone multifrequency [DTMF] confirmation) condition up to the number of times defined as the retry limit. If the user entered an address restricted by the switch, the attempt is counted as a retry failure.

Other Failures	The number of DTT call attempts where the call could not be completed. A failure can indicate that a message became stale or that the user entered an address restricted by the restriction/permission list (RPL) assigned to DTT.
Average Wait Time (mm:ss)	The average amount of time that the DTT service had to wait during the reporting period to acquire a channel to make the outcall.
Maximum Wait Time (mm:ss)	The longest amount of time that the DTT service had to wait during the reporting period to acquire a channel to make the outcall.
Blocked Attempts	The number of DTT attempts that were blocked due to the unavailability of channels.

Is the service being used?

Check the number of new requests. A low number can indicate minimal use of the DTT service. This can be caused by lack of awareness of the service among users, or lack of knowledge of how to use the service.

A low number of requests can also indicate a very restrictive RPL. Since the address is checked when the message is composed, a request is not made if the number is restricted.

Suggested actions

- Find out if users know about the feature and how to use it.
- If necessary, provide users with additional training.
- Requests are denied if the telephone number is restricted. Check the restriction/permission list assigned to DTT/DTF in your mailbox classes and check NCOS, TGAR, and CLS settings on the switch to make sure that delivery to the required external phone numbers is allowed.

- If the restricted numbers are appropriate, inform users of the restricted numbers to which they are not allowed to address messages.

Are messages being delivered?

Compare the number of successes to the number of new attempts. If the number of successes is lower than the number of attempts (or there is a high number of failures), messages are not being delivered.

Suggested actions

- Check the DTT setup in Outcalling Administration.
  - Make sure the economy delivery time overlaps with the allowed delivery times.
  - Make sure the stale time setting is not causing messages to become too old too soon.
- Check the average wait time, maximum wait time, and blocked attempts to see if the DTT service is having problems acquiring channels.
- Check the retry failures to see if the DTT retry limits are causing delivery failures.
- Check if the RPL assigned to DTT was changed. If the logon session allows a user to compose a message to an address but the RPL is later changed, the request fails and is logged under Other Failures.

Are allocated channel resources adequate?

High values in the following fields can indicate that the current channel allocations for the DTT service are insufficient for the amount of traffic DTT is generating:

- Average Wait Time
- Maximum Wait Time
- Blocked Attempts

Suggested actions

Increase the minimum or maximum number of channels, or both, allocated to the DTT service. Do this in the SDN Table by modifying the outbound SDN assigned to DTT. If you do not have enough channels to handle the traffic, you might have to purchase additional channels or change the allocations for other services.

Are retry limits appropriate?

If the number of retry failures is high, the retry limits for DTT might be too low.

Suggested action

Increase the DTT retry limits that are defined in Outcalling Administration.

DTT Audit Trail Summary Report

How to use this report

Use this report to determine which call attempts are responsible for the high retry counts and failures detected by the DTT Activity Report.

Report data

Name	The name of the mailbox owner.
Mailbox	The mailbox number from which the call originated.
Date	The date the call was made.
Time	The time the call was made.
Duration (hh:mm:ss)	The duration of the call in hours, minutes, and seconds.
Target Phone Number	The telephone number that was called.
Call Status	The result of the call in a numeric return code: **4** = Operation successful **14** = Could not reach destination: The phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **18** = Voice parts of message delivered; fax parts exist but were not delivered **19** = Fax parts of message delivered; voice parts exist but were not delivered **22** = Invalid destination number or bad/invalid address

Retry Counter	The total number of retry attempts that were made at the time of the call attempt. This field increments by one each time a retry attempt is made.

DTT Audit Trail Detail Report

How to use this report

Use this report to monitor Delivery to Telephone (DTT) usage by mailbox.

Report data

Name	The name of the mailbox owner.
Msg ID	The identification number of the message.
Target Phone Number	The telephone number that was called.
Date	The date the call was made.
Time	The time the call was made.
Duration (hh:mm:ss)	The length of the call in hours, minutes, and seconds.
Call Retries	The total number of retry attempts that were made. This field increments by one each time a retry attempt is made.
Process Type	One of the following audit trail entry types displays: **1** = Server process. This could be a submission of a new request, the rescheduling of a request, or the removal of a request. **2** = Agent made a call. **3** = Agent attempted to make a call but failed. This could be due to restriction/permission settings, problems with the switch (for example, no dial tone) or configuration.

Call Status	The result of the call in a numeric return code: **4 =** Operation successful **14** = Could not reach destination: The phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **18** = Voice parts of multimedia msg delivered; fax parts exist but were not delivered **19** = Fax parts of multimedia msg delivered; voice parts exist but were not delivered **22** = Invalid destination number or bad/invalid address
Action	The action performed on the request: **1 =** Reschedule **2** = Remove **3** = Add
Reason	Why an action occurred, in a numeric code: **1** = Answer limit exceeded **2** = Busy limit exceeded **3** = No answer limit exceeded **4** = End of period **5** = User logon **6** = RN disabled **7** = New message arrival **8** = Delivery OK **9** = Delivery failed **10** = Message deleted **11** = Message read **12** = Invalid DN
Channel Number	The DN of the channel used to place the call.

Fax Deliveries Activity Report

How to use this report

This report monitors Delivery to Fax (DTF) and fax printing activity over a specified time period. This means you get reports on fax deliveries to non-mailbox numbers (Delivery to Fax) as well as fax callback numbers entered by callers who have accessed services created with Application Builder that contain Fax Send blocks. In this last instance, the DTF service is also used to deliver the faxes to callers. Use this report to determine

- how much these services are being used
- if messages are being delivered
- whether the DTF service is able to acquire channels when needed
- whether the DTF retry settings are adequate

Additional information

You can print this report as a graph.

Report data

Date/Time Period	The date and time interval of the specified reporting period.
New Requests	The total number of new requests for fax delivery that were made during the reporting interval. A request is counted whenever a user tries to forward a fax to a mailbox, or a telephone number that is not a mailbox, or when a caller into an Application Builder service requests that a fax be delivered to a callback number.

New Attempts	The total number of attempts made to process the new requests for DTF and fax printing services during the specified time period.
Retries	The number of times that the DTF service retried delivering faxes that could not be delivered. DTF retries fax delivery when the destination fax device is busy or there is no answer, or when there is a transmission failure.
Successes	The total number of successful fax deliveries during the specified time period.
Retry Failures	The number of times that faxes could not be delivered because the retry limit was reached or exceeded. The system retries delivery attempts if the destination fax machine is busy or does not answer, if the connection cannot be made, or if there is a transmission error. If the target fax number is restricted by the switch, the attempt is counted as a retry failure.
Other Failures	The number of times faxes could not be delivered for reasons other than retry failures. A failure logged in this field can indicate that a fax became stale or that the target fax number is restricted in the RPL.
Average Wait Time (mm:ss)	The average amount of time the system waited to acquire a channel to deliver faxes.
Maximum Wait Time (mm:ss)	The longest amount of time the system had to wait to acquire a channel to deliver a fax.
Blocked Attempts	The number of fax delivery attempts that were blocked because channels were not available.

Are the services being used?

Check the number of new requests. If the number is low, callers might not be aware that the service exists, or they might not understand how to use the feature. Also, there could be a hardware or software problem.

A low number of requests can indicate a very restrictive RPL. Since the address is checked when the message is composed, a request is not made if the number is restricted.

Suggested actions

- Make sure the prompts recorded for the Application Builder service are worded clearly.
- Look for ways to promote the applications to users and callers (in the case of Application Builder services).
- Requests are denied if the fax number is restricted. Check the restriction/ permission list assigned to DTT/DTF in your mailbox classes and check NCOS, TGAR, and CLS settings on the switch to make sure that delivery to the required external fax numbers is allowed.
- If the restricted numbers are appropriate, inform users of the restricted numbers to which they are not allowed to send faxes.
- If the Application Builder service has been restored from backup, make sure the service has been opened, checked, and saved. Otherwise, callers hear an error prompt.
- Investigate technical problems and correct the situation.

Are messages being delivered?

If the number of successes is lower than the number of new attempts (or there is a high number of failures), faxes are not being delivered.

Suggested actions

- Check the DTF setup in Outcalling Administration.
  - Make sure the economy delivery time overlaps with the allowed delivery times.
  - Make sure the stale time setting is not causing faxes to become too old too soon.
- Check the average wait time, maximum wait time, and blocked attempts to see if the DTF service is having problems acquiring channels.
- Check if the RPL assigned to DTT/DTF was changed. If the logon session allows a user to send a fax to a particular fax number but the RPL is later changed, the request fails and is logged under Other Failures.
- Check the retry failures to see if the DTF retry limits are causing delivery failures or if there are indications of problems with the destination device.

Are allocated channel resources adequate?

High values in the following fields may indicate that the current channel allocations for the DTF service are insufficient for handling the amount of traffic DTF is generating:

- Average Wait Time
- Maximum Wait Time
- Blocked Attempts

Suggested actions

- Increase the minimum or maximum number of channels allocated to the DTF service. Do this in the SDN Table by modifying the outbound SDN assigned to DTF (and Multicast DTF, which is used to send broadcast fax messages).
- If you do not have enough channels to handle the traffic, you might have to purchase additional channels or change the allocations for other services.

Are retry limits appropriate?

Check the number of fax retries. Large numbers of retries indicate there were problems making a connection to the destination fax machine (busy, no answer, no carrier, transmission error).

Suggested actions

- To determine specific instances of high retries, run the Fax Audit Trail Summary Report for the corresponding time interval to see if the causes are due to no carrier or transmission errors (see “Fax Print Audit Trail Summary Report” on page 174). If this is the case, contact the organization to which you are sending faxes and ask them to examine their equipment.
- Consider increasing some of the retry limits that are configured in Outcalling Administration.

Fax On Demand Audit Trail Summary Report

How to use this report

This report provides summary information about Delivery to Fax calls placed by Application Builder services with fax callback capability. Use this report to investigate potential fax delivery problems that certain services are experiencing. For example, the Fax Deliveries Activity Report alerts you to the fact that a significant number of fax deliveries were unsuccessful due to retry failures. You can generate the Fax on Demand Audit Trail or the Fax Deliveries Activity Report to get details such as the called DN and the reason for the retry failure (no carrier versus transmission problems, for example).

Use this report to troubleshoot

- problems with an Application Builder service
- problems with a particular fax device
- the cause of lengthy fax delivery sessions

Report data

Date	The date of the fax delivery.
Time	The time of the fax delivery.
Duration (hh:mm:ss)	The length of the call in hours, minutes, and seconds.
Target Phone Number	The destination DN (fax phone number) of the call.
Call Status	The result of the call, in a numeric return code: **4** = Operation successful **6** = Protocol error

Call Status (continued)	**14** = Could not reach destination: the phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **18** = Voice parts of message delivered; fax parts exist but were not delivered **19** = Fax parts of message delivered; voice parts exist but were not delivered **22** = Invalid destination number or bad/invalid address **23** = Local system error
Successful Delivery	Whether the fax was successfully delivered (Yes or No).
Service DN	The Service Directory Number (SDN) of the Application Builder service from which a caller requested fax delivery to a callback number.
App Name	The name of the service (application) from which a caller requested fax delivery to a callback number. **Note:** The App Name only shows the current information associated with the Service DN. This information might not match the App Name at the time the call is made due to changes in the Service DN application or the application’s session profile.
Billing DN	The billing directory number of the application that originated the call. **Note:** The Billing DN only shows the current information associated with the Service DN. This information might not match the Billing DN at the time the call is made due to changes in the Service DN application or the application’s session profile.

Is there a problem with an Application Builder service?

If callers are requesting faxes from a particular service and faxes are regularly not delivered, there could be a problem with the service setup.

Check the Successful Delivery field for calls that were not successful. Then check the SDN and App Name fields to see whether faxes requested from particular services are not being delivered.

Suggested action

Check the session profile of the Application Builder service (accessible from the SDN Table). If the page transmission error handling is set to Quit, then faxes are not delivered if there is an error. Set this option to Continue to allow the service to retry transmission.

Is there a problem with a particular fax device?

Faxes sent to a particular fax device might not be delivered if there is a problem with the receiving fax device. The fax machine could be out of paper or turned off, for example.

Check the Successful Delivery field for calls that were not successful. Then check the Target Phone Number field to see if failed deliveries are associated with the same DN(s).

Suggested actions

- Contact the owner of the called DN to identify whether there is a problem with the destination device.
- Run the Fax On Demand Audit Trail Detail Report.

Are there any lengthy sessions?

Check the Duration field for fax delivery sessions that are especially long. A long session might indicate that hackers have gained access to an Application Builder service with fax callback capability and are using it to send faxes to pay-per-call numbers.

Suggested actions

- Take the Application Builder application out of service until the problem is fixed.
- Reduce the session time limit in the service’s SDN configuration.
- Follow up to see if the called DN is a pay-per-call number. If so, report your findings to the system administrator.
- If the service allows toll calls, consider assigning a more restrictive restriction/permission list to the service.
- Consider using password blocks to require callers to enter passwords before entering callback numbers that incur long distance charges.

Fax On Demand Audit Trail Detail Report

How to use this report

This report traces the fax delivery process from the outcall request to the final outcome. Use it to help you determine why a specific fax delivery attempt has failed. The results and the reason for the failure are provided.

Report data

Target Phone Number	The target DN of the fax delivery attempt.
Msg ID	The unique number the system assigned to each Delivery to Fax request. This allows all requests to be tracked.
Date	The date of the fax delivery attempt.
Time	The time of the fax delivery attempt.
Duration (hh:mm:ss)	The length of the call in hours, minutes, and seconds.
Service DN	The Service DN of the service from which the callback fax call originated.
Call Retries	The total number of retries for this request that have been made since the first attempt to deliver the fax. After each attempt, the counter increments by one. (The first attempt is considered retry 0.)
Process Type	The type of audit trail entry: **1** = Server process. This could be a submission of a new request, the rescheduling of a request, or the removal of a request. **2** = Agent made a call.

Process Type (continued)	**3** = Agent attempted to make a call but failed. This could be due to restriction/permission settings, problems with the switch (for example, no dial tone), or configuration.
Call Status	The result of the call, in a numeric return code: **4** = Operation successful **6** = Protocol error **14** = Could not reach destination: the phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **18** = Voice parts of message delivered; fax parts exist but were not delivered **19** = Fax parts of message delivered; voice parts exist but were not delivered **22** = Invalid destination number or bad/invalid address **23** = Local system error
Action	The action performed on the request: **1** = Reschedule **2** = Remove **3** = Add
Reason	Why an action occurred: **1** = Answer limit exceeded **2** = Busy limit exceeded **3** = No answer limit exceeded **4** = End of period **5** = User logon **6** = Disabled **7** = New message arrival

Reason (continued)	**8** = Delivery OK **9** = Delivery Failed **10** = Message Deleted **11** = Message Read **12** = Invalid DN
Channel Number	The DN of the channel used to place the call.

Fax Print Audit Trail Summary Report

How to use this report

This report tells you whether problems are with particular fax machines or are associated with particular mailboxes. Use it to determine which fax printing attempts are causing high retry counts and failures. This report is used with the Fax Print Audit Trail Detail Report.

Report data

Date	The date of the fax printing attempt.
Time	The time of the fax printing attempt.
Duration (hh:mm:ss)	The length of the call in hours, minutes, and seconds.
Target Phone Number	The DN of the fax device to which the fax was sent for printing.
Call Status	The call in a numeric return code: **4** = Operation successful **6** = Protocol error **14** = Could not reach destination: the phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **18** = Voice parts of message delivered; fax parts exist but were not delivered **19** = Fax parts of message delivered; voice parts exist but were not delivered

Call Status (continued)	**22** = Invalid destination number or bad/invalid address **23** = Local system error
Successful Delivery	Whether the fax was successfully printed (Yes or No).
Name	The first and last name of the user who printed the fax.
Mailbox	The number of the mailbox from which the print request originated.

Is there a problem with a particular fax machine?

Check the Target Phone Number field to see if printing problems are occurring with the same fax DN.

Suggested actions

- Test the fax machine associated with the DN to see if there are problems.
- To explore the cause of the problems in greater detail, run the Fax Print Audit Trail Detail Report (see “Fax Print Audit Trail Detail Report” on page 176).

Fax Print Audit Trail Detail Report

How to use this report

This report traces the fax delivery process from the print request to the final outcome. Use it to help you determine why a specific fax print delivery attempt failed. The results and the reason for the failure are provided. This report is available only if Multimedia Messaging is enabled on your system.

Report data

Target Phone Number	The number of the fax machine to which the fax was sent for printing.
Msg ID	The identification number assigned to the fax for tracking purposes.
Date	The date of the printing attempt.
Time	The time of the printing attempt.
Duration (hh:mm:ss)	The length of the call in hours, minutes, and seconds.
Mailbox	The number of the mailbox that requested fax printing.
Call Retries	The total number of retries for this request that have been made since the first attempt. After each attempt, the counter increments by one.

Process Type	The type of audit trail entry: **1** = Server process. This could be a submission of a new request, the rescheduling of a request, or the removal of a request. **2** = Agent made a call. **3** = Agent attempted to make a call but failed. This could be due to restriction/permission settings, problems with the switch (for example, no dial tone), or configuration.
Call Status	The result of the call in a numeric return code: **4** = Operation successful **6** = Protocol error **14** = Could not reach destination: the phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **18** = Voice parts of message delivered; fax parts exist but were not delivered **19** = Fax parts of message delivered; voice parts exist but were not delivered **22** = Invalid destination number or bad/invalid address **23** = Local system error
Action	The action performed on the request. The possibilities include **1** = Reschedule **2** = Remove **3** = Add

Reason	Why an action occurred: **1** = Answer limit exceeded **2** = Busy limit exceeded **3** = No answer limit exceeded **4** = End of period **5** = User logon **6** = Disabled **7** = New message arrival
Reason (continued)	**8** = Delivery OK **9** = Delivery Failed **10** = Message Deleted **11** = Message Read **12** = Invalid DN
Channel Number	The DN of the channel used to place the call.

Are there recurring fax printing failures?

Repeated failures to print faxes could indicate problems with the channel hardware. Look at the Channel Number field to determine which channel was acquired to print the fax. If the same DN keeps recurring along with printing failures, this can indicate channel problems.

RN Activity Report

How to use this report

This report can help you to determining Remote Notification (RN) busy times. Use it to obtain information about Remote Notification activity during a specified time period.

Use this report to troubleshoot

- low usage of the remote notification feature
- problems with restriction/permission lists applied to remote notification
- inadequate channel allocations for the service

Report data

Date	The date of the specified period.
Time Period	The time of the specified period.
New Requests	The number of new RN requests during the specified time period.
Retry Failures	The number of RN attempts that failed because the user did not log on to listen to new messages before the retry limit was exceeded. This can indicate one of the following situations: ■ The notification could not be delivered because the retry limit was exceeded and RN for that message stopped. ■ The notification was delivered, but the user did not log on to listen to the new message. ■ The target DN is restricted on the switch.

Other Failures	The number of RN attempts that failed due to reasons other than retry failures. A failure can occur if ■ The RPL assigned to DTF was changed after an RN request was accepted. ■ A notification request occurs outside the allowed time period.
Average Wait Time (mm:ss)	The average amount of time, in minutes and seconds, it took the RN service to acquire channels to place notification calls during the specified time period.
Maximum Wait Time (mm:ss)	The longest amount of time, in minutes and seconds, it took for the RN service to acquire a channel to make a call.
Blocked Attempts	The total number of times that an RN attempt was blocked because a channel could not be acquired.

Is the service being used?

A low number in the New Requests field can indicate low use of the RN service. This might be due to a lack of awareness of the service among users or a lack of knowledge of how to use the service.

A low number of new requests can also indicate that the RN server is out of service or not working.

Suggested actions

- Find out if users know about the feature and how to use it. You might need to provide users with additional training.
- Check the status of the RN server.

Are there excessive RN failures?

If the number of failed requests or other failures is high, notifications are not getting to users, and there could be a technical or setup problem.

Failures can indicate that the RPL assigned to RN changed after users set up their target DNs.

Suggested actions

- A high number of failures can indicate that RN to pagers is not working because of the pager setup. Check the pager configuration in your mailbox classes.
- Contact your pager company. They might not have enough lines to handle the volume of pager requests.
- Check the average wait time, maximum wait time, and blocked attempts to see if the RN service is having problems acquiring channels.
- If the RPL assigned to RN was changed, inform users of the numbers that are now restricted so that they can update their target DNs.
- Run the RN Audit Trail Summary Report to isolate specific instances of failure (see “RN Audit Trail Summary Report” on page 183).

Are allocated channel resources adequate?

High values in the following fields can indicate that the current channel allocations for the RN service are insufficient for the amount of traffic RN is generating:

- Average Wait Time
- Maximum Wait Time
- Blocked Attempts

Suggested actions

Increase the minimum or maximum number of channels or both, allocated to the RN service. Do this in the SDN Table by modifying the outbound SDN assigned to RN. If you do not have enough channels to handle the traffic, consider purchasing additional channels or changing allocations for other services.

RN Audit Trail Summary Report

How to use this report

Use this report to determine which Remote Notification (RN) attempts are responsible for the high number of failures detected by the RN Activity Report.

Use this report to troubleshoot

- which call attempts are responsible for high recounts and failures
- whether there are problems with users' RN setup

Report data

Name	The name of the user to which the RN was made.
Mailbox	The mailbox number from which the RN attempt originated.
Date	The date of the call.
Time	The time of the call.
Duration	The duration of the call in minutes and seconds.
Target Phone Number	The telephone or pager number that the mailbox called. This is the target DN that is defined in the user's RN setup.

Call Status	The result of the call, in a numeric return code: **4** = Operation successful **14** = Could not reach destination: the phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **22** = Invalid destination number or bad/invalid address
Retry Counter	The total number of retries for this RN request that have been made since the first attempt. After each attempt, the counter increments by one. RN attempts are retried if, for the first attempt, the target DN is busy, not answered, or answered without the user logging on to listen to new messages.

Which calls failed?

Determine which call attempts are responsible for the high retry counts and failures.

Suggested action

Run the RN Audit Trail Detail Report to see the details of each request submitted by the RN service (see “RN Audit Trail Detail Report” on page 186).

Are there problems with users’ RN setup?

If calls that originate from certain mailboxes keep failing, there could be problems with the way users have set up their RN service.

Suggested actions

- Check the Mailbox field to see if there are repeated RN failures from the same mailbox. The user might have selected the wrong device type in his or her RN setup or entered the wrong PIN (if notification is to a pager). Check the user’s RN setup in User Manager, or ask the user to verify the device type and PIN in his or her RN setup.
- Check the Target Phone Number field to see if there are repeated RN failures to certain phone numbers. If so, the target DN defined by the user might be invalid. From User Manager, check the user’s RN setup. Phone the target DN to see what happens. If you confirm that the number is not valid, contact the user and ask him or her to change or delete the target DN.
- Check the user’s RN setup from User Manager to determine if the time period is defined for too narrow a time.

RN Audit Trail Detail Report

How to use this report

This report is typically run after the RN Audit Trail Summary Report. Use it to see the details of each request submitted to the Remote Notification (RN) service.

Use this report to troubleshoot

- unusual traffic patterns
- users not receiving RNs

Report data

Name	The mailbox owner’s name.
Msg ID	The identification number assigned to the message for tracking purposes.
Target Phone Number	The telephone number that the mailbox called.
Date	The date of the call.
Time	The time of the call.
Duration	The duration of the call in minutes and seconds.
Call Retries	The total number of retries for this RN request that have been made since the first attempt. After each attempt, the counter increments by one. RN attempts are retried if, for the first attempt, the target DN is busy, not answered, or answered but the user does not log on to listen to new messages.

Process Type	One of the following audit trail entry types is displayed: **1** = Server process. This could be a submission of a new request, the rescheduling of a request, or the removal of a request. **2** = Agent made a call. **3** = Agent attempted to make a call but failed. This could be due to restriction/permission settings, problems with the switch (for example, no dial tone), or configuration.
Call Status	The result of the call, in a numeric return code: **4** = Operation successful **14** = Could not reach destination: the phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **22** = Invalid destination number or bad/invalid address
Action	The action performed on the request: **1** = Reschedule **2** = Remove **3** = Add

Reason	Why an action occurred: **1** = Answer limit exceeded **2** = Busy limit exceeded **3** = No answer limit exceeded **4** = End of period **5** = User logon **6** = RN disabled **7** = New message arrival **8** = Delivery OK **9** = Delivery Failed **10** = Message Deleted **11** = Message Read **12** = Invalid DN
Channel Number	The DN of the channel used to place the call.

Are there unusual traffic patterns?

To check whether unusual traffic patterns are occurring, run the Channel Usage Report (see “Channel Usage Report” on page 100). You can also check the DSP hardware and switch terminal number status.

Are there failed RNs?

If users complain about not receiving RNs, complete the following actions to identify the potential cause:

- Call the target phone number yourself. If the number is not valid, contact the user and ask him or her to change or delete the target DN.
- Set up an RN to your phone, and listen to the call.

Chapter 11

Networking reports

In this chapter

Networking Activity Report

How to use this report

This report monitors the messaging network activity between the local site and remote sites within your messaging network. Use it to

- determine whether AMIS and Enterprise networking have access to sufficient channel resources for the networking traffic load
- determine the network message traffic levels to each remote site (server)
- identify high numbers of failed networking sessions
- identify high numbers of Non Delivery Notification (NDN) messages
- identify high numbers of undelivered messages
- identify times when remote sites are not available

Additional information

You can print this report as a graph.

Report data

Date	The date of the specified reporting period.
Time Period	The time of the specified reporting period.
Protocol	The networking protocol. Possible values are: ■ Enterprise ■ AMIS ■ VPIM ■ unknown
Messaging Server	The name of the remote server being monitored.

Messages Sent	The total number of messages sent (including ACK’s and NDN’s) to the specified remote server from the local site.
Messages Received	The total number of messages received (including ACK’s and NDN’s) from the specified remote server.
Connect Time (mm:ss)	The total connect time between the local and the remote site, in minutes and seconds.
Total Sessions	The total number of connection attempts with the specified remote server.
Failed Network Sessions	The total number of connections made with the specified remote server which later failed due to an error.
Blocked Attempts	The total number of connection attempts with the specified remote server that failed because a channel was not available at the local site.
Site Unavailable	The number of times a connection to the remote server failed because the network call was dropped (call not answered or busy tone) or the network protocol failed (no D tone after C tone).
NDN Messages Delivered	The total number of NDN messages sent to remote site because messages could not be delivered to mailboxes at the local site.
Undelivered Messages	The total number of messages that could not be delivered to the remote server before the message stale timer expires.

Notes:

1. Several messages may be sent within one session.
2. Several sessions may be required to successfully deliver a message.

Does the network have sufficient capacity?

Check the Blocked Attempts field. A large number of blocked attempts can indicate that a channel was not available.

Suggested actions

- Check the SDN table to see if a maximum channel limit has been placed on AMIS or Enterpise networking services. If so, increase the maximum.
- Install additional channels.
- Run this report with an interval that extends from midnight to midnight over a typical business day. The graph shows the total network connect time for each hour of the day.
- Compare the connect times for the busiest hour to the maximum possible connect time (60 minutes for each channel times the maximum channels allowed for AMIS or Enterprise in the SDN Table).
- The ratio of the connect time to maximum possible connect time is an approximate estimate of the probability that an inbound or outbound network attempt will be blocked.
- If the ratio exceeds 40 percent, consider increasing the maximum channels for AMIS or Enterprise in the SDN table. If it is already set to the maximum, then consider adding more voice channel capacity to the local site.

Identify high numbers of failed sessions

Check the Failed Network Sessions field. A large number of failed sessions can indicate insufficient channel capacity at the remote site for handling the incoming networking calls.

Suggested actions

- Increase the maximum channels for AMIS or Enterprise in the SDN table. If it is already set to the maximum, then consider adding more voice channel capacity to the local site.
- Install more channels.

Identify high numbers of NDN messages

Check the NDN Messages Delivered field. A large number indicates that messages sent by local users are not being received by remote users. This could indicate incorrect configuration problems at the remote site.

Suggested actions

- Check your configuration.
- Alert the remote site’s administrator.

Identify high numbers of undelivered messages

Check the Undelivered Messages field. A message is undelivered when a successful networking session to a remote site cannot be established before the message stale time expires. A large number of undelivered messages can indicate networking problems at the remote site.

Suggested actions

- Adjust the stale time configuration.
- Alert the remote site’s administrator. If multiple sites are experiencing the same problem, the local site’s networking is the likely source of the problem.

Identify times when remote sites are not available

Check the Site Unavailable field. A large number of unavailable site occurrences indicates that a network call was dropped or the protocol failed.

Open Networking Activity Report

How to use this report

This report shows the messaging networking activity of the local site to open remote sites. Use it to determine how efficiently your system is working. The information contained in the report indicates if your system is properly configured for the system traffic or if it requires modifications.

An open remote site is not included in your network database and is not considered part of the integrated messaging network. AMIS Networking and VPIM Networking are the networking solutions that can exchange messages with open sites.

Note: Networking activity to integrated sites that are part of your messaging network is shown in the Networking Activity Report.

Use this report to check the number of

- blocked session attempts
- Nondelivery Notifications (NDN) and undelivered messages
- failed networking sessions

Additional information

You can print this report as a graph.

Report data

Date	The date of the specified period.
Time Period	The time of the specified period.
Protocol	AMIS or VPIM Networking.

Messages Sent	The total number of messages sent through open networking.
Messages Received	The total number of messages received through open networking.
Connect Time (hh:mm:ss)	The total connect time used by open networking sessions in hours, minutes, and seconds.
Completed Sessions	The total number of completed open networking sessions.
Failed Sessions	The total number of failed open networking sessions.
Blocked Session Attempts	The total number of blocked session attempts with the specified remote site.
Site Unavailable	The number of times an outgoing session was attempted with an available port, but the session could not be established because the remote site was not responding.
NDN Messages Delivered	The number of NDN messages returned to the local site.
Undelivered Messages	The total number of messages that were not delivered. An undelivered message occurs when a successful networking session to the remote site cannot be established before the message stale timer expires.

Identify high numbers of blocked sessions

Check the number of blocked session attempts. A large number can indicate that additional channels should be allowed for AMIS Networking.

Suggested action

Consider increasing the maximum channels for AMIS in the SDN table.

Identify high numbers of NDNs

Check the number of NDNs and undelivered messages. If the number of NDNs delivered or the number of undelivered messages is high, there could be a problem with your networking setup or with the switch/telephone network. Since Open AMIS requires the user to enter the DN to dial at the destination messaging system, the user might be addressing messages incorrectly.

Suggested action

Refer to the appropriate networking implementation and administration guide for details on the proper setup of the networking features in your system.

Identify high numbers of failed networking sessions

Check the number of failed networking sessions. A high number can indicate problems between sites.

Suggested action

Contact your system administrator and the administrator of the site you are trying to reach.

Chapter 12

Bill-back reports

In this chapter

800 Access Bill-back Report

How to use this report

Use this report to monitor 800 service use. Each call over an 800 facility to a specific mailbox is captured by name, mailbox, and department to allow easy billing.

Additional information

- You can export this report to a file format that you can use with an external bill-back program.
- If you set Department or Mailbox as the primary sorting criterion for this report, the Length Subtotal field appears in the printed report.

Report data

Date	The date of the 800 call.
Time	The time of the 800 call.
Length (sec.)	The length of time of the call, in seconds.
Called DN	The VSDN that the call was terminated on.
Session Type	The type of session that the call originated from: VM—Voice Messaging MM—Multimedia Messaging EVM—Express Voice Messaging SAM—Speech Activated Messaging CA—Call Answering FCA—Fax Call Answering EFM—Express Fax Messaging

Last Name	The last name of the mailbox owner.
First Name	The first name of the mailbox owner.
Mailbox	The mailbox number.
Department	The department of the mailbox owner.
Mailbox Class	The Class of Service (COS) of the mailbox.
Switch Location	The name of the switch location.

DTT Usage Bill-back Report

How to use this report

Use this report to bill back the cost associated with telephone activity to the appropriate user or department.

Additional information

- You can export report to a file format that you can use with an external bill-back program.
- If Department or Mailbox is specified as the primary sorting criterion for this report, the Call Hold Time Subtotal field appears in the printed report.

Report data

Name	The name of the user.
Mailbox	The mailbox number of the user.
Department	The department of the user.
Date	The date of the telephone call.
Time	The time of the telephone call.
Call Hold Time (hh:mm:ss)	The length of time that the user was on hold, in hours, minutes, and seconds.
Target DN	The directory number that is being called.
Retry Counter	The number of retries made to complete the call.
Mailbox Class	The Mailbox Class to which the user belongs.
Switch Location	The name of the switch location.

Messaging Usage Bill-back Report

How to use this report

Use this report to bill back the cost associated with telephone activity to a user based on the messaging activity of his or her mailbox. This report shows the total connect time and the new message time used by the specified mailbox.

Additional information

- You can export this report to a file format that you can use with an external bill-back program.
- If Department is specified as the primary sorting criterion for this report, the Session Length Subtotal field appears in the printed report.

Report data

Name	The name of the mailbox owner.
Mailbox	The mailbox to which the messaging activity is billed.
Department	The department to which the mailbox belongs.
Session Length (sec.)	The total length of time, in seconds, that the mailbox was used in Logon, Call Answering, or Visit Messenger sessions. If your system has submailboxes, a summary of connect time appears in the report.
Mailbox Class	The class of service to which the mailbox is assigned.
Switch Location	The name of the switch location.
Total Storage (kbytes)	The total amount of disk space used by the mailbox, in kbytes.
Date	The session start date.

Network Usage Bill-back Report

How to use this report

Use this report to record the networking activity of users that resulted in long distance charges. This report is normally generated as an ASCII file that can be used with an external bill-back program.

Use these results to bill back Reporter networking usage. The bill-back price structure can be based on time of day, duration, delivery location (remote site ID), priority, and billing class. Networking messages and non-delivery notifications (NDN) are not reflected in this total.

Report data

Last Name	The last name of the mailbox owner.
First Name	The first name of the mailbox owner.
Mailbox	The mailbox to which the networking activity is billed.
Date	The date of the networking session.
Time	The time of the networking session.
Duration (hh:mm:ss)	The length of the logon session in hours, minutes, and seconds.
Messaging Server	The CallPilot server being monitored.
Priority	The priority of the networking session.
Mailbox Class	The class of service to which the mailbox assigned.
Department	The department associated with the mailbox.
Switch Location	The name of the switch location.

RN Usage Bill-back Report

How to use this report

Use this report to bill the cost of outcalling activity by mailbox. Each record in this report is a Remote Notification (RN) or Delivery to Telephone (DTT) call made by the specified mailbox.

Additional information

If Department or Mailbox is specified as the primary sorting criterion for this report, the Call Hold Time Subtotal field appears in the printed report.

Report data

Name	The name of the mailbox owner.
Mailbox	The mailbox to which the report is billed.
Department	The department number of the active mailbox.
Date	The date that the call was answered.
Time	The time that the call was answered.
Call Hold Time (hh:mm:ss)	The length of the call, in hours, minutes, and seconds.
Target DN	The phone number that was the destination of the call.
Retry Counter	The number of retries made to complete the call.
Mailbox Class	The class of service to which the mailbox is assigned.
Switch Location	The name of the switch location.

Fax on Demand Bill-back Report

How to use this report

Use this report to charge the cost of Fax on Demand usage to the appropriate user or department.

Additional information

If Service DN (SDN) is specified as the primary sort criterion for this report, the Call Hold Time Subtotal field appears in the printed report.

Report data

Service DN	The application directory number.
Billing DN	The directory number to which the bill is sent.
Date	The date of the fax.
Time	The time of the fax.
Call Hold Time (hh:mm:ss)	The length of time of the fax in hours, minutes, and seconds.
Target DN	The DN (phone number of the fax machine) that was the intended destination of the fax call.
Retry Counter	The number of retries at the time of the attempt. This field is incremented by one each time a call fails to deliver the fax items requested.

Call Status	This field displays the result of the call, in a numeric return code: **1** = Could not reach destination: line busy **2** = Destination did not answer the call **3** = Unknown status **4** = Operation successful **5** = Protocol error (time-out, invalid data received, remote system aborts session) **6** = Call was answered by a human; also detected no fax carrier **7** = Voice parts of message delivered; fax parts exist but were not delivered **8** = Fax parts of message delivered; voice parts exist but were not delivered **9** = Invalid destination number; also site unreachable **10** = System error; unable to initiate outcalling session **11** = The destination DN is restricted **12** = The outcall was answered and the target device was notified **13** = All DNs in the user’s RN setup are invalid **19** = Fax parts of message delivered; voice parts exist but were not delivered

Fax Print Bill-back Report

How to use this report

Use this report to bill mailbox users for the long distance charges incurred by printing faxes to fax machines.

Additional information

If Department or Mailbox is specified as the primary sorting criterion for this report, the Call Hold Time Subtotal field appears in the printed report.

Report data

Name	The name of the user.
Mailbox	The number of the mailbox.
Department	The number of the department to which the user belongs.
Date	The date on which the faxback call was answered.
Time	The time at which the faxback call was answered.
Call Hold Time (hh:mm:ss)	The length of the faxback call in hours, minutes, and seconds.
Target DN	The phone number of the fax machine that was the intended destination of the fax call.
Retry Counter	The number of retries at the time of the attempt. This field is incremented by one each time a call fails to deliver the fax items requested.

Call Status	The result of the call in a numeric return code: **4** = Operation successful **6** = Protocol error **14** = Could not reach destination: the phone number dialed is busy **15** = Destination did not answer the call **17** = Long silence detected **18** = Voice parts of message delivered; fax parts exist but were not delivered **19** = Fax parts of message delivered; voice parts exist but were not delivered **22** = Invalid destination number or Bad/Invalid Address **23** = Local system error

Chapter 13

Alert reports

In this chapter

Failed DTT Alert

How to use this alert

The Delivery to Telephone (DTT) service allows users to send messages to telephone numbers that do not have mailboxes.

Set a threshold for this alert if you want to be notified of failed message deliveries. This alert is triggered if the percentage of failed DTT attempts exceeds the specified threshold.

Note: Thresholds are set using the CallPilot Reporter program. For more information, see “Setting a threshold for an alert” on page 56.

Alert data

Date	The date of the failures.
Time Period	The time of the failures.
New Arrivals	The number of new requests that were made to the DTT service during the time period.
Cancelled by Retry Limits	The number of DTT attempts canceled due to exceeded busy, no answer, or answered (no Dual-tone Multi-frequency confirmation) retry limits or because the message became too old.
Cancelled by Other	The number of DTT attempts that were canceled for other reasons. For example, DTT attempts could have been canceled if no channels were available.
Total Failed	The total number of DTT outcalls that failed due to retry or other causes. This number, taken as a percentage of the total DTT outcalls, triggers the alert if the predefined threshold is exceeded.

Investigate possible causes of failure

A high number of failed DTT sessions can indicate a problem with the DTT service setup.

Suggested actions

To identify why DTT attempts are failing, run the following reports to get more detailed information about DTT call sessions:

- “DTT Activity Report” on page 154
- “DTT Audit Trail Summary Report” on page 158
- “DTT Audit Trail Detail Report” on page 160

See Chapter 10, “Outcalling reports.”

Failed RN Alert

How to use this alert

The Remote Notification (RN) service notifies users of new messages in their mailboxes. The RN service calls the user at a remote phone or pager, as defined by the user. This service is enabled on a per mailbox class basis.

Set a threshold for this alert if you want to be notified of failed notifications. This alert is triggered if the percentage of failed RN attempts exceeds the specified threshold.

Note: Thresholds are set using the CallPilot Reporter program. For more information, see “Setting a threshold for an alert” on page 56.

Alert data

Date	The date of the alert.
Time Period	The time period covered by the alert.
New Arrivals	The number of new requests that were made to the RN service during the time period.
Cancelled by Retry Limits	The number of RN attempts canceled due to exceeded busy, no answer, or answered (no DTMF confirmation) retry limits or because the message became too old.
Cancelled by Other	The number of RN attempts that were canceled for other reasons. For example, RN attempts might have been canceled if no channels were available.
Total Failed	The total number of RN outcalls that failed due to retry or other causes. This number, taken as a percentage of the total RN outcalls, triggers the alert if the predefined threshold is exceeded.

Investigate possible causes of failure

A high number of failed RN sessions can indicate a problem with the RN service setup.

Suggested actions

To identify why RN attempts are failing, run the following reports to get more detailed information about RN call sessions:

- “RN Activity Report” on page 179
- “RN Audit Trail Summary Report” on page 183
- “RN Audit Trail Detail Report” on page 186

See Chapter 10, “Outcalling reports.”

RN Target Problem Alert

How to use this alert

Remote notifications (RNs) are sent to target telephone or pager numbers (DNs) that are defined in users' schedules. This alert notifies you of target DNs that the RN service cannot successfully reach. This can happen if, for example, a user has defined an invalid number.

Set a threshold for this alert if you want to be notified of problems with defined target DNs. This alert is triggered when the number of failures to a particular target phone number exceeds the specified threshold.

Note: Thresholds are set using the CallPilot Reporter program. For more information, see "Setting a threshold for an alert" on page 56.

Alert data

Target DN	The DN was not reached successfully.
Date	The date of the notification failure.
Time	The time of the notification failure.
Name	The owner of the mailbox from which the RN attempt originated.
Mailbox	The number of the mailbox.

Investigate possible causes of failures

Too many failed outcalls to an RN target can indicate an invalid target, a paging service outage, an RN setup problem, or user unresponsiveness.

Suggested actions

- If the failures are associated with one mailbox, contact the user and ask him or her to verify the target DN. Either you or the user must modify the current DN that is defined in the user’s schedule.
- If the failures to an RN target are associated with many mailboxes, this can indicate an outage at the paging service, a problem between CallPilot and the paging service, or user unresponsiveness. To test whether the paging service is at fault, call the service manually to see if it issues a page.
- If the pager service appears to be working correctly, then run the RN Audit Trail Detail Report to isolate the cause of the failures (see “RN Audit Trail Detail Report” on page 186).

Failed Networking Sessions Alert

How to use this alert

This alert is useful for determining whether your CallPilot system is experiencing hardware or setup problems, or has insufficient capacity on either the local or the remote site.

Set a threshold for this alert if you want to be notified of network messaging failures. This alert is triggered when the percentage of message failures equals or exceeds the specified threshold.

Note: Thresholds are set using the CallPilot Reporter program. For more information, see “Setting a threshold for an alert” on page 56.

Alert data

Messaging Server	The identification of the remote site where one or more networking calls failed.
Date	The date of the networking failure(s).
Time Period	The time of the networking failure(s).
Messages Attempted	The total number of networking messages attempted to a particular site for the given period since the last download of information.
Messages Failed	The total number of failed messages because the site could not establish a network session to a particular site in the time period specified.
Percent Failed	The percentage of failed calls to the number of total attempted calls to a particular site.

Investigate possible causes of failures

Too many failed network sessions indicates a networking hardware problem, a setup problem, or a lack of modem capacity on the remote site.

Suggested actions

- Run the Networking Activity Report to obtain more information about the problem (see “Networking Activity Report” on page 190).
- If failures are associated with one remote site, contact the site’s administrator. There can be a problem with the site’s networking setup or hardware.

Failed Fax Delivery Alert

How to use this alert

An attempt to deliver a fax is considered a failure if the complete fax item is not delivered to the target DN.

Set a threshold for this alert if you want to be notified of unsuccessful fax deliveries. This alert is triggered when the percentage of failures to a particular target fax number (DN) exceeds the specified threshold.

Note: Thresholds are set using the CallPilot Reporter program. For more information, see “Setting a threshold for an alert” on page 56.

Alert data

Date	The date of the fax delivery problem.
Time	The time of the fax delivery problem.
Service DN/Mailbox	If the fax originated from a mailbox this indicates the mailbox number. If the fax originated from an Application Builder service, this indicates the SDN of the service.
Target DN	If the fax originated from a mailbox, this indicates the target fax number to which the user sent the fax. If the fax originated from an Application Builder service, this indicates the fax callback number entered by the caller.
Channel DN	The channel number being used for the failed fax delivery.

Investigate possible causes of failures

Failed fax deliveries can be due to user error, such as incorrect keying of the fax number. Too many failed fax delivery sessions can also indicate a setup problem with fax services such as Delivery to Fax.

Suggested actions

- Call the target DN to ensure that a fax modem is used to answer the call (fax modems issue a carrier tone that is audible). Other error possibilities are a busy signal or that the fax carrier is not available because the fax machine is out of paper, not turned on, or out of order.
- If most of the failures are associated with one channel, there can be a hardware problem. Run diagnostics on the channel to determine whether this is the case. If so, contact technical support.
- If the problem does not seem to be related to the target DN or the channel, run the following reports to help isolate the cause of failures:
    - “Fax Deliveries Activity Report” on page 162
    - “Fax On Demand Audit Trail Summary Report” on page 167
    - “Fax On Demand Audit Trail Detail Report” on page 171
    - “Fax Print Audit Trail Summary Report” on page 174
    - “Fax Print Audit Trail Detail Report” on page 176

See Chapter 10, “Outcalling reports.”

Excessive After-Hours Logons Alert

How to use this alert

Hackers try to gain access to mailboxes and other system resources during nonbusiness hours, when their activity is less noticeable.

Set a threshold for this alert if you want to be notified of a high number of logons that occur after hours. This alert is triggered if the number of after-hours logons exceeds the specified threshold.

Note: Thresholds are set using the CallPilot Reporter program. For more information, see “Setting a threshold for an alert” on page 56.

Additional information

Before you can use this alert, you must specify the hours during the day that your company considers after-hours, or nonbusiness hours. After-hours are defined using the CallPilot Reporter program. For more information, see “Changing the alert hours” on page 79.

Alert data

Mailbox	The mailbox associated with the after-hours logon.
Date	The date of the after-hours logon.
Time	The time of the after-hours logon.
Duration (hh:mm:ss)	The length of the logon session in hours, minutes, and seconds.

Caller DN	The telephone number from which the logon originated. This field can contain four digits (mailbox), five or six digits (trunk group and member number), the last seven digits of a telephone number, or asterisks (*) if the data coming from the switch is null.

Identify potential hacker activity

Check whether logons are being made to a particular mailbox or a number of mailboxes. If the number of logons is very high or the duration of the logon sessions is long, hackers might have gained access to some mailboxes on your system. These can be unused mailboxes hackers are using for themselves or to gain access to thru-dial capabilities. Hackers can, for example, set up a single session over the evening to sell long-distance services.

Suggested actions

- Enable Hacker Monitor to monitor either the suspicious caller DN (referred to as a CLID in Hacker Monitor) or the mailbox. Whenever there is a thru-dial or logon from the CLID or mailbox, an alarm is generated to notify you.
- Check the status of the mailbox and its owner. Is the user actively using the mailbox, or is the user on vacation, or extended leave, or no longer with your company?
  - If the mailbox is unused because the user is no longer with your organization, delete the mailbox immediately. Hackers target unused mailboxes.
  - If the user is temporarily away, you can either change the user’s password or disable the mailbox until the user returns.
  - If the mailbox is active, ask the user if he or she is logging on frequently during off-hours. If the user is not the one logging on, inform him or her of the situation and request an immediate password change. Give the user tips on how to create secure passwords.

- Monitor the mailbox regularly.

Excessive Thru-Dialer Access Alert

How to use this alert

Hackers break into messaging systems to access thru-dial resources. They can then place long distance calls from your system at your expense.

Set a threshold for this alert if you want to be notified of a high number of thru-dials being placed from your system. This alert is triggered if the number of thru-dials exceeds the specified threshold.

Note: Thresholds are set using the CallPilot Reporter program. For more information, see “Setting a threshold for an alert” on page 56.

Alert data

Date	The date of the alert.
Time Period	The time period of the alert.
Number of Incoming Calls	The number of incoming calls that placed thru-dials during the time period.

What is the source of thru-dials?

If hackers are using your system for its thru-dial capabilities, you must identify how they are accessing thru-dial. Thru-dials can be made in a number of ways, and this alert provides only a single total that does not consider how the thru-dials are made. The following features allow users and callers to make thru-dials:

- Mailbox Thru-Dial
- Call Answering/Express Messaging Thru-Dial
- Application Builder services that contain Thru-Dial blocks

Are thru-dials originating from mailboxes?

Do the following to determine whether thru-dials are originating from mailboxes:

- Enable Hacker Monitor to monitor all mailboxes for thru-dials. This gives you a list of mailboxes with which to work.
- Enable Hacker Monitor to monitor those mailboxes that you suspect hackers are using for thru-dial services.
- If you suspect a hacker is using a mailbox to thru-dial, check the status of the mailbox. Is the user actively using the mailbox, or is the user on vacation, extended leave, or no longer with your company?
    - If the mailbox is unused because the user is no longer with your organization, delete the mailbox immediately. Unused mailboxes are targets of hackers and must be removed.
    - If the user is temporarily away, you can either change the user’s password or disable the mailbox until the user returns.
    - If the mailbox is active, ask the user to change the password immediately. Give the user tips on how to create secure passwords. For more information, see “Tips for creating secure passwords” on page 227.
    - Monitor the mailbox regularly.
- Check the restriction/permission list (RPL) that is assigned to the following features. You might need to assign a more restrictive list to prevent unauthorized toll calls.
    - Mailbox Thru-Dialing (RPLs are assigned in mailbox classes)
    - Call Answering/Express Messaging thru-dial (the RPL is assigned in Security Administration)

Are thru-dials from services?

Do the following to determine whether thru-dials are originating from Application Builder services:

- Run the Building Block Summary Report, and make sure Thru-Dial is the block type that will be reported on (see “Building Block Summary Report” on page 148). You can then identify how many times the Thru-Dial blocks in your Application Builder services have been accessed.
- Enable Hacker Monitor to monitor thru-dials from the Application Builder services or from all services you suspect hackers are using.
- Check the services you suspect to identify the restriction/permission list that is assigned. You can assign a more restrictive list to prevent unauthorized thru-dials.

Excessive Incomplete Messaging Accesses Alert

How to use this alert

One of the most common ways for hackers to gain access to a system is to guess mailbox numbers. However, hackers often enter many invalid mailbox numbers before finding one that is correct. Keep track of the number of invalid mailbox numbers that are entered over a certain interval to help alert you to potential hacker activity.

Set a threshold for this alert if you want to be notified when an excessive number of invalid mailbox numbers has been entered. This alert is triggered when the number of invalid mailbox numbers exceeds the specified threshold.

For more information, see “Setting a threshold for an alert” on page 56.

Alert data

Date	The date of the failed logons.
Time Period	The time of the failed logons.
Total Voice Mail Accesses	The total number of voice mail accesses to CallPilot. This number includes successful and unsuccessful logons.
Number of Logon Sessions	The total number of successful logons.
Failed Accesses	The total number of failed logons.
Percentage Failed	The percentage of all logons that failed.

Suggested actions

Do as much as you can to increase the security of all mailboxes on your system.

- In Security Administration, check your mailbox security settings to ensure that these precautions are in place:
  - A password prefix has been defined that becomes part of the default password for newly created mailboxes.
  - An acceptable minimum password length is defined (no less than six characters is recommended).
  - Users must change their passwords.
  - Users cannot reuse the same password until they have used several other passwords first.
  - Mailboxes are temporarily locked when a certain number of invalid logon attempts are made.

  For more information about the settings in Security Administration, see the Administrator’s Guide.

Tips for creating secure passwords

Secure passwords are hard for hackers to guess; remind all mailbox owners to follow these rules when creating passwords:

- Never use words that are in a dictionary. Combinations of letters and numbers are more difficult to guess.
- Never use your name or other personal information, such as your birth date or phone number.
- Never use family names, names of your pets, or other words that can be associated with you.
- Never let anyone borrow your password.
- Never write down your password.
- Never reuse old passwords.
- Use at least six characters in your password.

If you suspect a large-scale attack on many of your mailboxes, you can temporarily disable external logons until you get the situation under control. This is also done in Security Administration.

For more information about the settings in Security Administration, see the Administrator’s Guide.

Excessive Failed Logons Alert

How to use this alert

One of the most common ways for hackers to penetrate a system is to guess passwords. However, hackers often enter many invalid password before finding one that is correct. Keep track of the number of incorrect passwords entered over a certain interval to help alert you to potential hacker activity.

Set a threshold for this alert if you want to be notified of an excessive number of failed logons. This alert is triggered when the number of failed logons exceeds the specified threshold.

For more information, see “Setting a threshold for an alert” on page 56.

Alert data

Date	The date of the failed logon.
Time	The time of the failed logon.
Mailbox	The mailbox with the failed logon attempt.
Caller DN	The number that originated the attempt.

Suggested actions

Do as much as you can to increase the security of all mailboxes on your system.

- In Security Administration, check your mailbox security settings to ensure that these precautions are in place:
  - A password prefix has been defined that becomes part of the default password for newly created mailboxes.
  - An acceptable minimum password length is defined (no less than six characters is recommended).

- Users must change their passwords.
- Users cannot reuse the same password until they have used several other passwords first.
- Mailboxes are temporarily locked when a certain number of invalid logon attempts are made.

For more information about the settings in Security Administration, see the Administrator’s Guide.

Tips for creating secure passwords

Secure passwords are hard for hackers to guess; remind all mailbox owners to follow these rules when creating passwords:

- Never use words that are in a dictionary. Combinations of letters and numbers are more difficult to guess.
- Never use your name or other personal information, such as your birth date or phone number.
- Never use family names, names of your pets, or other words that can be associated with you.
- Never let anyone borrow your password.
- Never write down your password.
- Never reuse old passwords.
- Use at least six characters in your password.

If you suspect a large-scale attack on many of your mailboxes, you can temporarily disable external logons until you get the situation under control. This is also done in Security Administration.

For more information about the settings in Security Administration, see the Administrator’s Guide.

Index

CallPilot
Reporter Guide

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

The process of transmitting data and call messaging between the Meridian 1 and CallPilot is proprietary to Nortel Networks. Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

Publication number:	555-7101-310
Product release:	2.02
Document release:	Standard 1.0
Date:	May 2003