555-7101-301

CallPilot

Administrator’s Guide

Product release 2.02 Standard 1.0 May 2003

NORTEL NETWORKS™

CallPilot

Administrator’s Guide

Publication number:	555-7101-301
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 CallPilot server and the Meridian 1 switch or Succession CSE 1000 system 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

Standard 1.0 issue for CallPilot 2.02. The section “Configuring and troubleshooting Email-by-Phone” has been moved to this document from the *General Release Bulletin*. A note was added to the procedure for logging on to the CallPilot server and a minor update to the section on the impact on system performance.

October 2002

This is the Standard 1.0 issue of the *CallPilot Administrator’s Guide*.

Contents

Part 1 Getting started 15

5 Configuring dial-up access to the CallPilot server 149

Section A: Configuring pcAnywhere on a personal computer 153

Section B: Establishing a dial-up connection to the server 161

Part 2 Securing the CallPilot system 177

6 CallPilot security recommendations 179

7 Physically securing your equipment and data 183

8 Backing up and restoring CallPilot information 189

17 Using templates to create new mailboxes 329

18 Using mailbox classes to manage mailbox privileges 339

Part 5 Configuring service defaults 349

19 Configuring addressing conventions 351

20 Configuring messaging service defaults 365

Part 6 Monitoring the CallPilot system 455

Part 1

Getting started

In this part

Chapter 1

CallPilot administration overview

In this chapter

What’s new in CallPilot 2.02?

What is CallPilot?

CallPilot is a powerful unified messaging system that offers a single solution for managing many types of information, including

- voice, fax, and e-mail messages
- telephone calls
- calendars
- directories
- call logs

CallPilot users can send and receive both voice and fax messages through display-based phonesets, wireless sets, Windows desktop computers, or a speech recognition interface.

Major changes in CallPilot

- CallPilot administration over the Web
- Enhanced management of the messaging network
- Enhanced mailbox use from a mobile phoneset
- Enhanced mailbox use from a personal computer
- Enhanced backup and restore capabilities
- Easier delegation of administrative tasks
- Expanded search functionality
- Ease of use with other messaging solutions
- Enhanced addressing capability
- Succession CSE 1000 switch connectivity
- Symposium Voice Services Support

CallPilot administration over the Web

You no longer have to use a particular administrative PC to

- administer a CallPilot server
- generate reports about the CallPilot server

The Web application CallPilot Manager replaces the Windows-based CallPilot Administration client used in prior versions of CallPilot.

CallPilot Reporter has been converted to a Web application.

You can use any Windows personal computer running

- Internet Explorer 5.0 or later
- Netscape 6.2 or later

Note: Application Builder remains a Windows-based application. Administrators can use CallPilot Manager to download Application Builder and the CallPilot Player to a personal computer.

You use a web browser to	For detailed information, see
Monitor the CallPilot server.	Part 6, “Monitoring the CallPilot system”
Generate Operational Measurement (OM) reports.	“Running system reports” on page 463
Configure a CallPilot server.	Part 1 of the *CallPilot Installation and Configuration* binder, Chapter 2 “Installing, configuring, and maintaining CallPilot”
Grant full or specific administrative privileges to others without defining access classes.	■ “About CallPilot administration” on page 31 ■ Chapter 4, “Delegating administrative tasks”

You use a web browser to	For detailed information, see
Create and maintain a messaging network.	The CallPilot Manager online Help book Creating a messaging network.
Set security options for CallPilot Manager sessions.	The CallPilot Manager online Help topic Getting started → “Setting security options for CallPilot Manager sessions”.

Enhanced management of the messaging network

CallPilot 2.02 provides the CallPilot administrator with the ability to

- configure extensive network security enhancements
- configure network broadcast capability for mailbox class members
- automatically add a permanent remote user and record a spoken name on the user’s behalf
- configure time and date stamps on messages and voice prompts to be indicated in the user’s time zone, instead of in the time zone of the CallPilot server

Network security enhancements

Network security enhancements include

- encryption of message traffic using transport layer security (TLS)
- authentication of desktop messaging users and remote voice mail servers submitting messages to CallPilot
- monitoring of suspect SMTP network activity

For detailed information, refer to the following CallPilot Manager online Help books:

- Creating a messaging network → Encryption
- Creating a messaging network → SMTP security

Network broadcast capability

If networking or NMS is installed, you can permit selected mailbox owners to send location broadcasts or network broadcasts.

For detailed information, refer to the following CallPilot Manager online Help books:

- Creating a messaging network → Network and location broadcasts
- Creating a messaging network → Message delivery options

Network Message Service in multiple time zones

All switch locations can be located in the same time zone, or in different time zones from the CallPilot server (local site). If one or more switch locations are located in a different time zone from the CallPilot server, you should define the time zone for each location. This results in time and date stamps on messages and voice prompts to be indicated in the user’s time zone, instead of in the time zone of the CallPilot server.

For detailed information, refer to the following CallPilot Manager online Help books:

- Creating a messaging network → Switch locations
- Reconfiguring the CallPilot server → Configuring the CallPilot server

Creation of multiple remote mailboxes in a single operation

You can use the Auto Admin feature to create a group of remote mailboxes in a single operation. All mailboxes added as a group must be based on the same user creation template.

For detailed information, refer to the CallPilot Manager online Help book “Administering mailboxes at a remote location.”

Names Across the Network

A CallPilot feature that allows the spoken names of message senders to be reproduced at recipient sites. If a sender does not exist at the recipient site as a remote user, a temporary remote user is added to the site with the sender’s text name and spoken name.

Names Across the Network eliminates the need for a system administrator to manually add a permanent remote user and record a spoken name on the user’s behalf.

For detailed information, refer to the CallPilot Manager online Help topic Creating a messaging network → Messaging server sites and locations → “Configuring the local messaging server”

Enhanced mailbox use from a mobile phoneset

If speech activated messaging is installed, selected mailbox owners can use voice commands instead of key commands to use their CallPilot mailboxes.

CallPilot 2.02 speech activated messaging enhancements provide

- the “Goodbye, CallPilot” voice command
- easy switching between voice commands (speech activated messaging) and DTMF commands
- access to e-mail messages from a mobile phoneset

Goodbye, CallPilot

Mailbox owners can use the new voice command “Goodbye, CallPilot” to easily close their mailboxes when they are using a mobile phoneset.

No special configuration is required.

Easy switching between voice commands and key commands

Mailbox owners using speech activated messaging can simply press a key to switch to DTMF commands and back again. Refer mailbox owners to the *CallPilot Speech Activated Messaging User Guide*.

No special configuration is required.

Access to e-mail messages from a mobile phoneset

If the new keycoded feature E-mail-by-Phone (Text To Speech) is installed, you can provide mailbox class members with the ability to use voice commands to listen to their e-mail messages over a mobile phoneset in any of 10 languages.

See “Permitting mailbox class members to listen to e-mail messages over a phoneset” on page 347.

Enhanced mailbox use from a personal computer

Desktop messaging enhancements include

- mailbox use and management via My CallPilot from any personal computer running either Internet Explorer 5.0 or later, or Netscape 6.2 or later
- remote text notification of new or urgent messages

My CallPilot

The CallPilot desktop messaging license also permits each desktop messaging user to access My CallPilot.

My CallPilot is a suite of web-based applications for CallPilot mailbox owners. It provides a central graphical interface for managing messages, mailbox and messaging options.

My CallPilot includes

- *CallPilot Messages (also known as web messaging):* A section in the My CallPilot application for managing CallPilot and e-mail messages. It lets mailbox owners access their messages anywhere Internet access is available.
- *CallPilot Features:* A section in the My CallPilot application that enables mailbox owners to select and modify mailbox and messaging options.
- *Useful Information:* A section in the My CallPilot application that includes reference information and online guides for CallPilot mailbox owners.

The applications and features in My CallPilot that are available to mailbox owners is determined by the software installed on the system and privileges assigned by the CallPilot administrator.

For detailed information, refer to

- *CallPilot Desktop Messaging and My CallPilot Installation Guide*
- *CallPilot Desktop Messaging and My CallPilot Administration Guide*

Remote text notification

Remote text notification of new or urgent messages is provided with the basic CallPilot product. You can permit selected mailbox owners to use this new unified messaging component.

Note: When a CallPilot 1.07 system is upgraded to CallPilot 2.02, mailbox owners with remote notification capability are automatically given remote text notification capability.

For detailed information, see “Message notification options” on page 63.

Enhanced backup and restore capabilities

CallPilot Manager provides enhanced backup and restore capabilities as well as simplified processes. Both significantly reduce the workload for CallPilot administrators.

Dynamic archive capability

When you add or delete mailboxes or administrators, you do not have to manually add or delete them to or from a user archive that has been defined to store information that includes the new information. This is because the user archive backup process employs CallPilot Manager search functions to automatically update the archive as you back up information. See “Using mailbox (user) archives” on page 215.

Simplified processes

CallPilot 2.02 provides streamlined backup and restore processes.

You can	For detailed information, see
Back up the entire CallPilot system to a tape drive or to a remote disk drive on your LAN.	■ "Scheduling backups to tape or disk" on page 202 ■ "Performing an immediate backup to tape or disk" on page 207
Use the same process to back up ■ system configuration information ■ mailbox information ■ custom system prompts ■ custom applications and services	■ "Scheduling backups to tape or disk" on page 202 ■ "Performing an immediate backup to tape or disk" on page 207
Use CallPilot Manager to ■ Monitor the status of a backup or restore operation. ■ Review the details of a prior backup or restore operation.	"Monitoring the status of a backup or restore operation" on page 196
Define a user archive around any of the user search criteria.	"Using mailbox (user) archives" on page 215
Restore information archived for all deleted mailboxes only.	"Using mailbox (user) archives" on page 215

Easier delegation of administrative tasks

CallPilot 2.02 administrators need to set up and apply access classes before they can delegate administrative tasks.

CallPilot 2.02 administrators can immediately define any or all of the following types of administrator:

- *full administrator without mailbox:* A CallPilot Manager user without mailbox privileges. Typically, an offsite support technician.
- *global administrator:* A mailbox owner who has been granted access to all CallPilot Manager functionality.
- *specialized administrator:* A mailbox owner who has been granted access to specified CallPilot Manager functions.

  Typically, a specialized administrator is located at the customer site and performs ongoing maintenance such as resetting mailbox passwords and changing mailbox owner information. For example, you can grant any mailbox owner the right to reset passwords for other mailbox owners before you make the system available to your users.

For detailed information, see Chapter 4, "Delegating administrative tasks."

Expanded search functionality

Your ability to search for CallPilot mailbox information is expanded so that

- You can use a quick search, an advanced search or a saved search when you back up to, or restore from, mailbox (user) archives.
- You can base search criteria directly on the data elements that have been entered on the CallPilot server.

The Search Criteria list provides data elements (for example, mailbox number, last name, or first name) on which you can base search criteria. To facilitate location of the data element you need, the list is organized into groups that reflect the labels on user and mailbox property sheets, such as: General, DNs, Fax Options, and Remote Notification.

For detailed information, see Chapter 12, "Finding mailboxes, administrators, or directory entries," on page 281.

Ease of use with other messaging solutions

In addition to the default phoneset interface for callers and mailbox owners, CallPilot provides the following alternate phoneset interfaces:

- *CallPilot menu interface:* Commands for mailbox owners and callers provided by a voice menu defined as a custom application
- *CallPilot alternate command interface:* Voice prompts used by the organization’s alternate user interface.

For detailed information, see Chapter 21, “Configuring CallPilot services” Section D: “Configuring Symposium Voice Services support,” on page 415.

Enhanced addressing capabilities

CallPilot 2.02 provides the following addressing enhancements:

- support for mixed area/city codes
- enhanced broadcast capability
- support for pause characters and number signs in DN addresses

Support for mixed area or city codes

In high-density population areas, a call to an area with a different area code is often treated as a local call because new area codes are introduced to accommodate all the telephone numbers required for area residents. You can use CallPilot Manager to configure the CallPilot server to distinguish between local and long distance calls in high-density population areas.

Network broadcast capability

If networking or NMS is installed, you can permit selected mailbox owners to send location broadcasts or network broadcasts. See “Enhanced management of the messaging network” on page 20.

Support for pause characters and number signs

CallPilot 2.02 allows mailbox owners to use desktop messaging or My CallPilot to configure timed pauses and authorization or access codes within DN addresses.

Note: The phoneset interface does not support this enhancement.

You can use CallPilot Manager to include pause characters and required number signs in telephone and fax addresses, including the following special-purpose DNs:

- mailbox revert DN
- default Printing DN (fax-capable mailboxes only)
- remote notification DN

For detailed information, see

- *Desktop Messaging and My CallPilot Administration Guide*
- *My CallPilot User Guide*
- CallPilot Manager online Help topics listed when you look up **pause characters** in the index

Succession CSE 1000 switch connectivity

CallPilot 2.02 supports connectivity to the Succession CSE 1000 switch.

For detailed information, see the *CallPilot Installation and Configuration Guide* for your server platform.

Symposium Voice Services support

Symposium Voice Services support allows customers who install multiple keycoded unified messaging components (for example: fax messaging, desktop messaging and My CallPilot, or E-mail By Phone) to purchase a CallPilot system with integrated Symposium Voice Services features.

CallPilot provides the following functionality:

- full backward compatibility with current Meridian Mail Voice Services
- migration from Meridian Mail of voice prompts, as well as IVR and ACCESS ports

- new voice prompt editor

  CallPilot Application Builder will reside on the same server as Symposium Web Client 4.0.
- allocation of up to 95 CallPilot voice channels for Voice Services support

CallPilot System Administrator needs to maintain two sets of call channels:

- one set for regular CallPilot standard features
- one set for ACCESS voice item maintenance

For more detailed information, see Chapter 21, “Configuring CallPilot services” Section D: “Configuring Symposium Voice Services support,” on page 415.

What’s new about the documentation?

The CallPilot 2.02 documentation incorporates the following major changes:

- **The *CallPilot Installation and Configuration Planner* replaces the *CallPilot Getting Started* quick reference.**

  The new document provides planners and distributors with an end-to-end view of the CallPilot installation and configuration tasks to make a CallPilot system functional for a customer. The document is available both as a printed document and as a PDF file from the CallPilot Documentation CD. The PDF document contains hyperlinks to the installation and configuration procedures to which it refers.

- **CallPilot Manager online Help is the primary source of procedural information.**

  The *CallPilot Administrator’s Guide* provides more detailed conceptual information and instructions for locating relevant online Help topics.

ATTENTION

The only procedures detailed in this guide are those not included in CallPilot Manager online Help.

- **The *CallPilot Monitoring and Security for the Administrator* guide has been integrated into the *CallPilot Administrator’s Guide*.**

  The *CallPilot Administrator’s Guide* provides an end-to-end view of how to set up and configure a CallPilot system. It is available only in PDF format and contains only those procedures referenced in the *CallPilot Installation and Configuration Planner.* The *CallPilot Administrator’s Guide* (this guide) provides instructions for locating relevant online Help topics.

About CallPilot administration

Introduction

Once your switch is installed and provisioned and your CallPilot server is installed and configured, set up a very basic CallPilot system. After that has run smoothly over a period of routine maintenance, extend the system functionality to meet the requirements of your organization and users.

Local or remote administration over an IP connection

Typically, you administer and maintain the CallPilot server over an IP connection between the server and one or more personal computers. You log on to the server via a URL, with a userid (mailbox number) and a password.

You can use either of the following Web browsers to administer CallPilot:

- Internet Explorer 5.0 or later
- Netscape 6.2 or later

You can use Internet Explorer to administer CallPilot either at the local machine or from a personal computer on the customer LAN. If you want to use Netscape 6.2 to administer CallPilot, you must use a remote personal computer

ATTENTION Netscape must not be installed on the CallPilot server.

See also

See “Remote administration over a LAN or dialup connection” on page 32.

What is CallPilot Manager?

CallPilot Manager is the web-based application used to connect to a CallPilot server. Once you have connected to the server, you can create and maintain the information the server uses to provide CallPilot messaging services to authorized mailbox owners.

This information includes

- user groups and permissions
- system settings
- messaging service settings
- maintenance and diagnostics

See also

See “Logging on to the CallPilot server with CallPilot Manager” on page 122.

Remote administration over a LAN or dialup connection

In the event that your IP service is not available, you can use third-party software to control the CallPilot server over a dial-up connection or a LAN connection.

This guide includes instructions for using the Symantec Corporation product pcAnywhere for setting up remote administration at an administrator’s site.

One licensed copy of pcAnywhere Version 10.5 is provided for the server on the CallPilot server software CD. pcAnywhere Version 10.5 is also installed on the server at the factory.

ATTENTION

To install pcAnywhere Version 10.5 on the remote personal computer, you must purchase a separate license for the remote personal computer.

See also

Chapter 5, “Configuring dial-up access to the CallPilot server,” on page 149

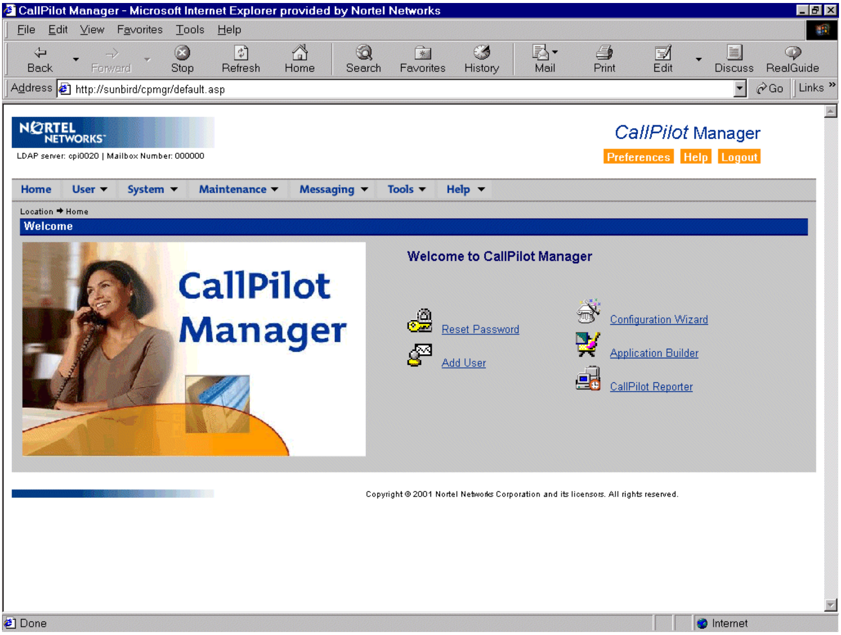
Delegation of administrative tasks

CallPilot Manager encompasses diverse functionality. The administrators who use it can be distributors, support technicians, or regular day-to-day administrators of customer systems.

When you use CallPilot Manager, you can delegate administrative tasks among different administrators. For example, you can set up your CallPilot system so that a user group administrator controls user access to CallPilot messaging services while a network administrator controls system configuration and backups.

CallPilot Manager administrator shortcuts

The CallPilot Manager home page includes shortcuts for tasks that CallPilot administrators perform regularly, such as adding a user or resetting a mailbox password. The shortcuts that appear depend on the CallPilot Manager functions that you are permitted to use.


CallPilot Manager - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss RealGuide
Address http://sunbird/cpmgr/default.asp
Go Links
NORTEL NETWORKS
LDAP server: cpi0020 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location ➜ Home
Welcome
CallPilot Manager
Welcome to CallPilot Manager
Reset Password
Add User
Configuration Wizard
Application Builder
CallPilot Reporter
Copyright © 2001 Nortel Networks Corporation and its licensors. All rights reserved.
Done
Internet

For example, shortcuts to Reset Password and Add User appear only if you have User Administration rights.

See also

Chapter 4, “Delegating administrative tasks,” on page 133

About this guide

Introduction

The *Administrator's Guide* provides the information you need to

- set up user and messaging administration of a CallPilot system
- perform frequent or routine administrative tasks
- extend the functionality of a CallPilot system
- system monitoring and troubleshooting information

See also

"Related information products" on page 37

Assumptions

This guide assumes that

- the CallPilot server has been correctly installed and is operational
- the switch has been installed and provisioned to support your CallPilot system

If the CallPilot server has not been installed, then install it before proceeding. For installation instructions, refer to the CallPilot Installation and Configuration binder for your server model.

Skills you need

Switch technology experience or knowledge

Knowledge of, or experience with, one or more of the following products is recommended:

- Meridian 1 (M1) PBX equipment, X11 release 23c and greater
- Succession CSE 1000 equipment
- Microsoft Windows NT, 95, or 98

PC experience or knowledge

Knowledge of, or experience with, the personal computer used as the administrative PC is assumed. For more information on these products, please refer to the documentation provided by the manufacturer.

Other experience or knowledge

Other types of experience or knowledge that can be of use include

- network management
- client/server systems

Related information products

Introduction

The following CallPilot technical documents are stored on the CallPilot documentation CD 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

  The My CallPilot software contains a Useful Information area that provides access to the end-user guides in Acrobat PDF format.

Document titles	NTP number
Desktop Messaging and My CallPilot 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
Desktop Messaging and My CallPilot Administration 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

Document titles	CallPilot release	NTP number
VPIM Implementation and Administration Guide	1.0	555-7101-306

Note: The CallPilot 1.0 networking guides remain unchanged since CallPilot 1.0. For instructions on how to configure the networking services on CallPilot, refer to the CallPilot Manager online Help.

End user guides

The following guides are intended for CallPilot mailbox owners:

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 online Help for mailbox owners

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

Understanding CallPilot features and services

In this chapter

Overview

Introduction

This chapter describes the following key features, services, and capabilities available with CallPilot 2.02.

- built-in features, services, and capabilities
  - voice messaging and call answering services and features
  - outcalling services
  - addressing capabilities
  - message notification capabilities
  - backup and restore features and capabilities
- monitoring and security features
- mailbox administration capabilities
- keycoded features and services
  - networking
  - fax (multimedia) messaging
  - speech-activated messaging
  - desktop messaging and My CallPilot
  - E-mail by Phone
- Application Builder services

Section A: Built-in features and services

In this section

Overview

Introduction

Built-in CallPilot services do not must be purchased by the customer.

Additional CallPilot services include

- keycoded features and services
- custom services developed in Application Builder

See also

- Section D: “Keycoded features and services,” on page 105
- Section E: “Custom applications (Application Builder services),” on page 117

Security feature

Since you can control access to some built-in features and services, some configuration is required to make them available to mailbox owners and callers.

See also

- “Revert DN feature” on page 51
- “Call sender feature” on page 52

Voice messaging and call answering services

Introduction

All CallPilot mailboxes have voice messaging and call answering capabilities. Whenever callers dial a mailbox owner who does not answer the call, they reach the CallPilot mailbox and hear the voice prompt provided by the CallPilot call answering service. Typically, the mailbox number is the mailbox owner’s primary extension DN.

Call answering service

Call answering service provides the opportunity for a caller to leave a message for a mailbox owner who does not answer a call. Callers are presented with a greeting and then prompted to leave a message.

Voice messaging service

Voice messaging services provide all mailbox owners with the capability to compose, send, retrieve, and manipulate voice messages from a mailbox, by using commands entered on the phoneset keypad. Whenever callers dial the voice messaging service DN (SDN), they hear voice prompts.

In addition to playing messages, a voice messaging service enables mailbox owners and callers to do the following:

- Record greetings and a spoken name.
- Play message header information.
- Compose and send messages to mailboxes or telephones on or off the local CallPilot messaging network.
- Configure messages to be sent at a later time.

- Reply to a message (either to the sender or to the sender and all recipients) or forward it.
- Tag messages as urgent or private.
- Tag messages to request notification when the recipient has received or played the message.
- Send the caller to a human attendant (the revert DN feature).
- Call the sender of a message (the call sender feature).

Configuration requirements and options

The primary CDN configured on the switch is added to the SDN Table as the primary voice messaging service when CallPilot is installed. The installer can add other CDNs to the SDN Table either during installation or by running the Configuration Wizard at a later time.

Administrators with access to CallPilot Manager Service Directory Number functionality can do the following:

- Add additional voice messaging CDNs to the SDN Table as needed.
- Re-allocate channels to support resource management.

Custom prompts

CallPilot supplies a list of basic prompts for each language installed on the CallPilot server. If you install the CallPilot Player, CallPilot Manager Custom Prompts functionality can listen to the supplied prompts and customize them to suit your requirements.

Once a custom prompt is created, the prompts administrator can

- select either the supplied or the customized prompt
- edit the customized prompt as often as necessary

Controlling costs with dialing restrictions and permissions

To control telecom costs, you can configure different dialing permissions for different groups of mailbox class owners. An administrator with access to the CallPilot Manager Mailbox Classes functionality must apply, *for each mailbox class*, the appropriate restriction permission list (RPL) to the following voice messaging features:

- revert DN
- thru-dial
- call sender

Revert DN feature

The DN to which callers are forwarded when they press 0 during a messaging or call answering session is referred to as the revert DN. You might want to permit some mailbox owners to use the revert DN feature to place domestic or international long distance calls while restricting others to internal or local off-switch calls only.

Thru-dial feature

The thru-dial feature enables a mailbox owner, caller, or CallPilot service to transfer to another DN by dialing 0 followed by the DN.

Custom application developers can use the Application Builder Thru-Dial block to configure services that require the thru-dial process.

You might want to permit some mailbox owners, callers, or Application Builder services to use the thru-dial feature to place domestic or international long distance calls and restrict others to internal or local off-switch calls only.

Call sender feature

The call sender feature of the voice messaging service enables a mailbox owner using the default voice messaging phoneset interface to dial the sender of a voice message. The mailbox owner can press 9 during message playback to place a call to the sender. The call is placed if the calling line ID (CLID) is known and if the assigned RPL permits calls to the CLID. You might want to permit some mailbox owners to use the call sender feature to place domestic or international long distance calls and restrict other s to internal or local off-switch calls only.

Note: Call Sender is available from both the CallPilot telephone interface and desktop messaging.

Express voice messaging service

The express voice messaging service enables callers to leave a message directly in a CallPilot mailbox. The call does not ring the mailbox owner’s phoneset. Whenever callers dial the express voice messaging SDN, they are prompted to specify the mailbox number, and then to leave a voice message. An express voice messaging service can be configured to automatically send messages to a specific mailbox.

Express voice messaging service provides the following capabilities:

- It provides a shortcut to callers who want to leave a voice message to one or more mailbox owners.
- It enables callers who reach a human attendant to leave a message for a mailbox owner. The attendant conferences in the express voice messaging SDN and enters the desired mailbox number, and then drops out of the call.
- It enables callers who reach a voice menu to leave a message directly in a mailbox.
- It enables an administrator to set up a guest mailbox without associating it with a phoneset. A visitor to a site can collect messages without having a phoneset designated for his or her personal use.

Configuration requirements

The CDN or phantom DN configured on the switch as the express voice messaging service can be added to the SDN Table either when CallPilot is installed or at a later time by an administrator with access to CallPilot Manager Service Directory Number functionality.

Alternate phoneset interfaces

CallPilot can be configured to permit use of an alternate phoneset interface that is similar to a widely-used command-based or a widely-used menu-based phoneset interface. Use of either of these alternate interfaces means that you do not have to force mailbox owners who are accustomed to a different interface to learn unfamiliar phoneset commands.

ATTENTION

Since an alternative user interface supports only core messaging functions, the mailbox owner must use the CallPilot voice messaging interface, desktop messaging, or My CallPilot to access advanced fax (multimedia) messaging and mailbox administration functions.

The mailbox number

All alternate interface users must have mailbox numbers with the configured number of digits to allow logon by entering the mailbox and password as a single string of digits without the usual mailbox terminator (#) required for standard CallPilot. Although CallPilot mailbox numbers with fewer digits are accepted if mailbox owners supply the terminator, this is not recommended.

ATTENTION

Logons via an alternate phoneset interface to mailboxes with more than the defined number of digits fail because CallPilot assumes that all input received after the defined number of mailbox digits is part of the password.

Access control

A Session Profile setting in the SDN definition controls whether or not the SDN interface style overrides the mailbox owner’s preferred style. If this setting is disabled, callers to the standard Voice Messaging SDN are presented with the mailbox owner’s preferred phoneset interface (CallPilot menu interface or CallPilot alternate command interface) following initial access to the mailbox.

Configuration requirements and options

No special installation or switch configuration is required.

The following list describes CallPilot server configuration requirements and options:

1. An administrator with access to CallPilot Manager *Service Directory Number* functionality must configure CallPilot to present these new mailbox owners (following initial logon) with phoneset commands that are similar to those to which they are accustomed.
2. An administrator with access to CallPilot Manager *Messaging Management* functionality must configure the number of digits required for each mailbox configured to use an alternate phoneset interface.
3. An administrator with access to CallPilot Manager *Mailbox Classes* functionality must configure mailbox classes to enable mailbox owners to use either the CallPilot voice messaging interface or an alternate phoneset interface.
4. An administrator with access to CallPilot Manager *User Administration* functionality must ensure that the appropriate mailbox class is assigned to new and existing mailboxes.

See also

- Section C: “Configuring alternate phoneset interfaces,” on page 405
- “Configuring mailbox classes,” on page 343
- “Changing a mailbox owner's mailbox class” on page 302

Outcalling services

Introduction

Outcalling services use the connected switch to make calls to telephones or faxphones that are not associated with CallPilot mailboxes.

Outcalling services include

- delivery to telephone (DTT)
- delivery to fax (DTF)
- remote notification (RN)

ATTENTION

Outcalling services can enable mailbox owners to send voice or fax messages to external DNs on the public network. This means that these services can incur toll charges for the calls they make. You can apply restriction permission lists (RPLs) to control unauthorized charges.

Availability to customers

Outcalling services are provided with all CallPilot systems. Customers can use mailbox classes to enable outcalling services for specified mailboxes only.

Delivery to telephone

Enable delivery to telephone (DTT) for mailbox owners who must be able to compose and send voice messages to on-switch or off-switch DNs that are not associated with CallPilot mailboxes. CallPilot calls the number and then plays the message to the recipient, who has the opportunity to record a reply to the message.

Delivery to fax

Enable delivery to fax (DTF) for mailbox owners who must be able to print fax messages or send fax items to on-switch or off-switch DNs that are not associated with CallPilot mailboxes.

For example, sales staff may must fax product descriptions to customers.

Remote notification

Remote notifications can be sent to pagers or to telephones that are not associated with a CallPilot mailbox.

Enable remote notification (RN) for mailbox owners who must be informed of new or urgent CallPilot messages immediately, even when they are away from their office phonesets.

For example, all technical support staff must be able to be notified immediately whenever a message arrives at a help desk.

See “Message notification options” on page 63.

Addressing capabilities

Introduction

Callers use telephone numbers to address CallPilot mailboxes. CallPilot requires dialing information to translate a number into a dialable number (DN).

Dialing information

Dialing information consists of

- information required to dial out from the local switch and access a private (ESN) or public network
- information required to distinguish certain area/city codes which are used for either local calls or long distance calls, depending on the destination DN

CallPilot uses *dialing translation definitions* to determine how to treat DNs with mixed area or city codes. Mixed area or city codes can be either local or long distance for a location, depending on the exchange code.

Pause characters

Include a pause character in a DN to insert a 2-second pause between digits. Pauses are not supported for internal DNs.

You may require pauses in a dialable number

- to access an external line
- to wait for the recipient system to answer a call before entering an access code or mailbox number

In CallPilot Manager, you can use pause characters in the revert DN, default printing DN, or remote notification callback DN.

Note: The phoneset interface does not support entering pause characters.

Number sign support

Mailbox owners must include the number sign (#) in a dialable number to terminate entry of access codes or authorization codes that follow the PSTN.

CallPilot does not support the use of number signs in internal DNs.

In CallPilot Manager, you can use the number sign

- in the default printing DN
- in combination with pause characters

Configuration requirements

An administrator with access to CallPilot Manager *Messaging Management* functionality must configure dialing information.

See also

- “Specifying off-switch dialing prefixes” on page 352
- “Handling mixed area or city codes” on page 355

Addressing messages to non-mailbox numbers

Addressing messages to non-mailbox numbers is referred to as *outcalling*.

CallPilot outcalling services are

- delivery to telephone (DTT)
- delivery to fax (DTF)
- remote notification (RN)

Delivery to telephone

Delivery to telephone (DTT) is the CallPilot service that allows mailbox owners to compose and send voice messages to phonesets, whether or not they have mailboxes associated with them.

DTT replaces the Meridian Mail Delivery to Non-User (DNU).

Delivery to fax

Delivery to fax (DTF) is the CallPilot service that allows users to send faxes to internal or external faxphones.

Note: Before a mailbox owner can send or receive fax messages, fax capability (a keycoded feature) must be installed and the mailbox owner must belong to a mailbox class with fax capability enabled.

Configuration requirements

- An administrator with access to the CallPilot Manager *Outcalling Administration* functionality must configure the addressing prefixes and dialing codes for delivery to telephone (DTT) and delivery to fax (DTF).
- An administrator with access to the CallPilot Manager *Mailbox Classes* functionality must apply the appropriate restriction permission list (RPL) to each mailbox class.
- An administrator with access to the CallPilot Manager *User Administration* functionality must ensure that the appropriate mailbox class is assigned to each mailbox owner.

See also

- “Outcalling services” on page 55
- “Remote notification of new or urgent messages” on page 65
- “Monitoring and security features” on page 75
- “Changing a mailbox owner's mailbox class” on page 302
- “Configuring mailbox classes,” on page 343
- “Defining address prefixes for both DTT and DTF” on page 359

Addressing groups

For the purpose of sending a single message to a list of recipients, CallPilot supports

- personal distribution lists (PDLs)
- shared distribution lists (SDLs)

- broadcast messages

Personal distribution lists

When mailbox owners create personal distribution lists (PDLs) from their phonesets, those lists are available only to the creator. Each PDL allows the user to send a recorded message to all the mailboxes contained in the list. A mailbox owner can create up to 99 personal distribution lists, each containing a maximum of 200 addresses. An address can be, for example, a local or remote mailbox, a shared distribution list.

Shared distribution lists

Shared distribution lists (SDLs) are similar to PDLs, except that they are created by administrators. Maintaining a comprehensive list of SDLs optimizes your server’s capacity because it minimizes the need for mailbox owners to create their own PDLs.

ATTENTION

Each SDL adds one address to a message recipient list, regardless of the number of addresses in the SDL. Each PDL adds the total number of addresses in the PDL to a message recipient list. For example, an SDL with ten entries adds one address, while a PDL with ten entries adds ten addresses.

Configuration requirements

An administrator with access to CallPilot Manager *Mailbox Classes* functionality must set up mailbox classes that permit access to SDLs.

See also

Chapter 15, “Maintaining shared distribution lists”

Broadcast addresses

A mailbox owner uses a broadcast address to address a message that is intended for all recipients at the local server, another location, or in the entire messaging network.

Broadcast capability

CallPilot supports

- no broadcast capability
- local broadcast capability only
- both local broadcast and network broadcast (includes location broadcast) capability, if a networking solution is installed

Local broadcasts

A voice message that is delivered to all of the mailbox owners on the local system is called a local broadcast.

A mailbox owner uses a broadcast mailbox to send a message to all mailbox owners at the local site. The broadcast mailbox is automatically defined on CallPilot as 5555. An administrator with access to CallPilot Manager **Messaging Management** functionality can change the broadcast mailbox number

Location broadcasts

A voice message that is sent to all mailbox owners at a specific remote site or switch location in the messaging network is referred to as a location broadcast.

A mailbox owner specifies the location broadcast number when composing the message from a mailbox with broadcast capability.

Network broadcasts

A message that is sent to all mailbox owners at both local and remote sites (including switch locations) in the messaging network is referred to as a network broadcast.

A mailbox owner specifies the network broadcast number when composing the message from a mailbox with broadcast capability.

Configuration requirements

For local broadcasts:

- An administrator with access to CallPilot Manager *Messaging Management* functionality must define broadcast message numbers.
- An administrator with access to CallPilot Manager *Mailbox Classes* functionality must set up mailbox classes that permit local broadcast capability.
- An administrator with access to CallPilot Manager *User Administration* functionality must ensure that mailbox owners are assigned a mailbox class with local broadcast capability enabled.

For location and network broadcasts:

- Networking (a keycoded service) or Network Management Service (NMS) must be installed on the CallPilot server.
- Broadcast message capability must be enabled between the local CallPilot server and remote messaging servers.
- Remote messaging servers must run either Meridian Mail Release 12 or later, or CallPilot 2.0 or later.
- An administrator with access to CallPilot Manager *Mailbox Classes* functionality must set up mailbox classes that permit network broadcast capability.
- An administrator with access to CallPilot Manager *User Administration* functionality must ensure that mailbox owners are assigned a mailbox class with network broadcast capability enabled.

See also

- “Networking solutions” on page 107
- “Changing a mailbox owner's mailbox class” on page 302
- “Configuring mailbox classes,” on page 343
- “Defining the broadcast message numbers” on page 397

Message notification options

Introduction

CallPilot provides message notification options to address the following scenarios:

- The mailbox has a dedicated phoneset and DN.
- An assistant must sometimes use his or her phoneset to answer a manager’s telephone.
- The mailbox is associated with one of several DNs associated with a single phoneset. (Several mailbox owners share a phoneset.)
- The mailbox has no dedicated phoneset. (It might be a guest mailbox or a suggestion box It might support a helpdesk staffed by a team of individuals who take calls on their own phonesets.)
- More than one mailbox is associated with a single DN. (For example, there is a single phoneset extension for several workers on a shop floor. Workers can use express voice messaging to leave each other messages.

Methods of message notification

CallPilot supports the following types of notification of new messages:

- phoneset/desktop message waiting indication (MWI)
- remote voice message notification to a telephone
- remote text notification to an e-mail device

Note: MWI By DN is an X11 software feature introduced in Release 24. It allows configuration of phoneset keys to indicate waiting messages for each mailbox associated with a single phoneset. MWI DN is a useful option when mailbox owners have their own extensions but share a phoneset.

Phoneset and desktop message waiting indication

The message waiting indicator (MWI) is activated whenever the mailbox receives a message that meets the criteria specified in the message waiting indication options specified for the mailbox.

The MWI depends on the user interface:

- On a digital phoneset, the message waiting indicator lights up.
- On an analog phone, the dial tone may be stuttered.
- *If desktop messaging (a keycoded feature) is installed and enabled:* On the desktop, the message waiting indicator is an icon in the form of a red phone.

The MWI DN is the extension which indicates that a message is waiting.

Configuration requirements

MWI is configured for each mailbox. The default is to indicate all new messages.

- Before a group of new mailboxes is added to a CallPilot server, an administrator with access to CallPilot Manager *User Administration* functionality can configure the MWI setting (All New, All Urgent and Unsent, New Urgent, or None) in the user creation template
- To change MWI for an existing mailbox, an administrator with access to CallPilot Manager *User Administration* functionality must search CallPilot to display the mailbox properties and then change the setting.

See also

The CallPilot Manager online help topic “Changing message waiting indication for a mailbox”

Remote notification of new or urgent messages

Remote notification is a service that calls mailbox owners at a specified DN whenever new messages arrive in their mailboxes. This service is intended for people who must be aware of new messages immediately, such as doctors, salespeople, or support staff.

CallPilot can send notifications to other phonesets (a home or cell phoneset), or to pagers or paging services.

- If a mailbox owner is notified at another phoneset, he or she can use the same phoneset to log on to his or her mailbox and listen to the messages.
- If a mailbox owner is notified at a pager, he or she must log on to CallPilot to retrieve new messages.

Configuration requirements

RN is configured for each mailbox.It must be enabled in the mailbox class assigned to the mailbox.

- An administrator with access to CallPilot Manager *Mailbox Classes* functionality must
  - Enable remote notification capability.
  - Set default remote notification options for mailbox class members.
- Before a group of new mailboxes is added to a CallPilot server, an administrator with access to CallPilot Manager *User Administration* functionality can configure remote notification options that are common to the group, such as a notification retry strategy.
- After a group of new mailboxes is added to a CallPilot server, an administrator with access to CallPilot Manager *User Administration* functionality can override the options set for the group or configure individual information, such as the remote notification callback number.

See also

The CallPilot Manager online help topics “Setting remote notification options for mailbox class members” and “Configuring remote notification for a mailbox owner”

Remote text notification of new or urgent messages

Remote text notification is a service that sends an e-mail notification message to mailbox owners when new messages arrive in their mailboxes.

This service is intended for people who must be aware of new messages immediately, such as doctors, salespeople, or support staff.

CallPilot can send notification messages to any e-mail device that supports the SMTP protocol, including desktop e-mail clients, personal digital assistants (PDAs), and paging devices that support e-mail.

When mailbox owners receive a notification message, they can log on to CallPilot to retrieve new messages.

Configuration requirements

1. An administrator with access to CallPilot Manager *Messaging Management* functionality must configure a notification device class with service provider settings for any communications service that supports the SMTP protocol.

2. An administrator with access to CallPilot Manager *User Administration* functionality must configure the e-mail notification options for mailbox owners.

   - Before a group of new mailboxes is added to a CallPilot server, an administrator with access to CallPilot Manager *User Administration* functionality can configure e-mail notification options that are common to the group, such as enabling Wireless And E-mail MWI and specifying the notification device class.
   - After a group of new mailboxes is added to a CallPilot server, an administrator with access to CallPilot Manager *User Administration* functionality can override the options set for the group or configure individual information, such as the e-mail address of the mailbox owner’s e-mail account to be used for CallPilot message waiting indication

See also

For information about configuring remote text notification on the CallPilot server, refer to the following CallPilot Manager online help topic "Configuring remote text notification (e-mail notification of waiting messages)."

Backup and restore capabilities

Introduction

CallPilot Manager provides backup capabilities for full system backups and archives.

An administrator with access to CallPilot Manager *Backup and Restore* functionality can do the following:

- Use both backups and archives to copy data to tape or to disk.
- Back up and archive files to server tape or to a remote disk drive.
- Schedule backups and archives or perform them immediately.
- Restore archived information.
- Monitor the status of a backup or restore operation.

Full system backups

Perform full system backups frequently and at regular intervals to do the following:

- Save and restore a complete set of system and multimedia data files from your CallPilot server, in the event of disk drive failure or corrupted or lost configuration and messaging data.

- Protect against data loss due to theft or damage caused by natural disasters.

ATTENTION

Nortel Networks recommends that you schedule periodic backups (even on servers equipped with RAID):

- Backups protect against data loss due to software problems (for example, file system corruption, registry corruption, and failed upgrades), undetected disk errors, double faults, and human error.
- Backups and archives are useful for migration to a different CallPilot platform.

How IPE and tower and rackmount system backups differ

All IPE systems are shipped with one drive. Tower and rackmount systems are shipped in either of the two following configurations:

- a server with only one drive
- a server with three drives

If your tower and rackmount system has three drives, you can back up the entire system, or you can back up a specific drive. This option is useful if a drive will be replaced.

Restoring data from system backups

ATTENTION

Your distributor is responsible for using your backups to return the server to the state it was in when the backup was created.

Archives

Archives are copies of multimedia files from CallPilot. Archives specifically back up Application Builder applications, personal user data (such as greeting, messages, and personal distribution list), and customized voice prompts.

CallPilot supports the following archive types:

- *User archives* store all CallPilot configuration information about mailboxes, mailbox owners, and administrators.

ATTENTION You can select the information to include in a single archive by defining search criteria for the archive. You can also select archived mailbox information to restore.

- *Prompt archives* store all custom prompts recorded in a single language.

ATTENTION You cannot selectively restore customized prompts from a prompt archive.

- *AppBuilder archives* store custom applications created using Application Builder.

How an archive differs from a system backup

Use both backups and archives to copy data to tape or to disk. You can back up and archive files to server tape or to a remote disk drive. Both can be either scheduled or performed immediately.

Archives and full system backups differ with respect to purpose, limitations, and impact on the system.

Purpose

Archives	Full system backups
■ To support recovery from inadvertent deletions of a user’s messages or mailbox, personal distribution lists (PDLs), customized prompts, and custom applications. ■ To port custom applications from another system. ■ To port mailboxes and administrators from another system.	■ To save a complete set of system and multimedia data files from your CallPilot server in the event of disk drive failure or corrupted or lost configuration and messaging data. ■ To restore these files to return the server to the state it was in when the backup was created. ■ To protect your system against data loss due to theft or natural disasters.

Limitations

Archives	Full system backups
▪ Archives do not save switch-related setup, operational measurement data, event logs, alarms, system security settings, the networking setup, or queues of undelivered and time-delayed messages. ▪ If you restore one or more messages from a user archive, they are added to the messages currently in the destination mailbox. The mailbox owner may complain that deleted messages re-appear in the mailbox. ▪ You cannot selectively restore customized prompts from a prompt archive.	▪ You cannot perform or schedule a complete system backup to a local disk. ▪ You cannot selectively restore data from a system backup.

Impact on the system

Archives	Full system backups
You can restore data from an archive without taking the CallPilot system out of service.	Since backups compete with services for system resources, schedule backups to run during off-peak hours.

Configuration requirements

Before archives can be scheduled or performed, an administrator with access to CallPilot Manager *Backup and Restore* functionality must define the backup destination. Backup devices for full system backups are predefined.

To define a selective user archive, an administrator with access to CallPilot Manager *Backup and Restore* functionality must be familiar with

- guidelines for defining a set of user archives
- understand how to use the User Administration search functions

See also

- Chapter 8, “Backing up and restoring CallPilot information”

Section B: Monitoring and security features

In this section

Overview

Introduction

To manage system resources effectively, you must be able to monitor server performance and allocate channels in a multimedia environment.

CallPilot Manager provides the tools to monitor

- server performance
- call channels and multimedia channels
- CallPilot server disk space
- the CallPilot database

These monitoring tools include

- alarms
- events
- reports

Note: CallPilot Reporter provides the tools you must run system status reports.

See also

- Chapter 22, “Monitoring the CallPilot server and resources”

Finding information about the CallPilot server

Introduction

You can use CallPilot Manager to

- view server settings
- monitor server performance

Viewing server settings

You may need Server Settings information when you communicate with product support personnel.

The Server Settings information includes

- a list of features and services installed on the CallPilot server
- a resource list showing the capacity of the CallPilot server
- a description of the switch connected to the CallPilot server
- the serial port settings of the CallPilot server

Performance Monitor

Performance Monitor enables you to view the server’s operating conditions. You can use the information from this window to determine whether your system has sufficient processor capacity, memory, or storage space. You can also use this information to improve the efficiency of your system. For example, to improve daytime performance, you can reschedule events to run at night, when the server is not as busy.

Collecting information for system reports

The CallPilot Reporter feature provides the tools you must run system status reports.

You can use CallPilot Manager to configure the report data to collect. The administrator shortcuts on the CallPilot Manager home page provide a link to the Reporter program.

Running reports

The Reporter utility provides predefined reports to help you monitor service usage and performance. You can also create your own custom reports.

CallPilot Reporter

ATTENTION

Reporter and CallPilot Manager must be installed on the same server. For more information, refer to Part 4 of the *CallPilot Installation and Configuration* binder.

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 on-screen reports which you can then

- print on a daily, weekly, or monthly basis
- export to a variety of file formats
- customize for easier reading

Since CallPilot Reporter is web-based, no reports or operational measurement data are stored on a personal computer; they are stored on the CallPilot server.

Availability to customers

Reporter is packaged with the CallPilot software.

How to access Reporter

Access Reporter from any PC using a web browser.

You can view reports for one CallPilot server at a time in a particular web browser window. To connect to a second server and view reports for that server, you must open a second web browser window.

See also

- “Finding information about the CallPilot server” on page 461
- “Running system reports” on page 463
- *CallPilot Reporter Guide*

Monitoring channels

Introduction

If the CallPilot server has trouble processing incoming calls, use Channel Monitor to view the state of call channels.

Channel Monitor

From Channel Monitor, you can

- monitor the current activity of functioning call channels, and identify which call channels are not functioning
- identify a call channel’s physical location

You can identify a channel’s physical location by its icon’s position on the Channel Monitor page. Channel Monitor also displays a channel's directory number (DN) and position (Label) in a popup when you move the mouse cursor over the channel's check box.

Multimedia Monitor

From Multimedia Monitor, you can

- monitor the current activity of functioning call channels, and identify which call channels are not functioning
- identify a call channel’s physical location
- identify the media type associated with a channel (voice, fax, or speech recognition) and review multimedia resources allocation

An understanding of channel allocation can help you determine if you must reconfigure the channels or add MPC-8 cards to increase the multimedia processing capacity of the server.

You can identify a channel’s physical location by its position on the Multimedia Monitor page. Multimedia Monitor also displays a channel's directory number (DN) and position (Label) in a pop-up when you move the mouse cursor over the channel's check box.

See also

- “Monitoring call channels” on page 466
- “Monitoring multimedia channels” on page 468

Monitoring disk space

Introduction

This section describes the general steps to take to maintain an even distribution of data on your system hard disk so that it performs efficiently and to capacity.

The performance of your CallPilot system depends, to some degree, on the amount of available disk space. Without enough disk space, the server cannot perform adequately. In some circumstances, the server can stop functioning.

Nortel Networks systems are engineered to provide adequate space to meet your data storage and system operation requirements. You must, however, monitor disk space occasionally to ensure space does not become too limited.

Disk partitions

The CallPilot server is formatted in the following two disk partitions:

- The Multimedia File System (MMFS) contains messages and greetings and other changing CallPilot data.
- The database includes administrative information such as user profiles, which include user names and directory numbers, and operational measurements (OMs), which are raw data about the system.

What monitoring disk space involves

For the most part, monitoring disk space involves watching for alarms. You can, however, take a more active role by monitoring the following units of storage:

Nortel directory disk space

You can determine the percentage of free disk space for the fixed disk containing the Nortel directory using the Server Performance Monitor (SPM).

For more information on monitoring the Nortel directory disk space, see “Monitoring Nortel directory disk space” on page 472.

MMFS volumes

The MMFS volumes store all voice and fax messages, and other related multimedia files, such as user mailboxes, greetings, voice prompts, and voice menus.

Of all the disk space on the system, the MMFS volumes are most likely to fill up first. Monitor them frequently to determine any changes in usage patterns.

For more information on monitoring MMFS volumes, see “Monitoring Multimedia File System volumes” on page 473.

The database

The database stores all configuration information and statistics, such as the number of calls processed within a certain time period.

For more information on monitoring the database, see “Monitoring the database using alarms” on page 480.

Nightly audit

Each night, the CallPilot server performs an audit that cleans up expired files in the Multimedia File System and the system database.

In particular, the audit removes user messages from the MMFS that have passed their expiry date and expired OMs from the system database. You can configure how long OMs are stored.

See also

- “Monitoring Nortel directory disk space” on page 472
- “Monitoring Multimedia File System volumes” on page 473
- “General methods to monitor disk space” on page 476
- “Monitoring the database using alarms” on page 480

Monitoring the database

Introduction

The database stores user information, system configuration information, and various statistics that are collected by the system. You cannot monitor the database disk space directly. However, an alarm is raised if the database reaches its expected limit.

Viewing and filtering server events

Introduction

Events are occurrences on the CallPilot server, such as applications opening or closing, or errors being reported. These events appear in

- Windows NT Event Viewer on the server
- CallPilot Manager Event Browser and Alarm Monitor

Note: The Alarm Monitor does not report information-level events.

Events are categorized by severity, as described below.

System events

System events, such as Windows NT driver events, appear as event code 40592 in the Event Browser and in the system log in the Windows NT Event Viewer.

Security events

Security auditing is enabled on the server. Suspicious actions by a user are logged as event code 40593 in the Event Browser and in the security log in the Windows NT Event Viewer. This is an information event, so it does not appear in the Alarm Monitor.

See also

- Chapter 23, “Viewing and filtering server events”

Configuring mailbox security

Introduction

CallPilot Manager provides the tools for you to do the following:

- Define mailbox logon requirements for all system users.
- Enable and configure security options that control external logons and limit the number of unsuccessful logon attempts.
- Apply dialing restrictions and permissions both globally and selectively to avoid unauthorized telecom charges.

Mailbox security issues, recommendations, and guidelines

Chapter 11, “Maintaining restriction permission lists,” on page 257 of this guide provides detailed recommendations and guidelines for maintaining mailbox security.

Restriction permission lists

Certain services and custom applications are capable of placing calls outside your system onto the public network. This means they can be used to place long-distance calls that incur toll charges.

Use of restriction permission lists (RPLs) ensures that your organization can control toll charges and prevent unauthorized charges.

A restriction permission list (RPL) limits the DNs to which CallPilot applications can connect.

To adequately secure the CallPilot unified messaging system, RPLs must be applied to each of the following:

- the entire system (the global RPL)
- a mailbox owner group (mailbox class RPLs)

- an individual application or service (application-specific RPLs)

See also

- Chapter 10, “Configuring mailbox security,” on page 243
- Chapter 11, “Maintaining restriction permission lists,” on page 257
- “Recommendations and guidelines” on page 244
- “Controlling access to mailboxes” on page 251

Monitoring suspicious activity

Introduction

If you have noticed suspicious activity on your system, use CallPilot Security Administration features to monitor CallPilot for certain events that you suspect are caused by hackers who have gained access to your system. When the event you are monitoring occurs, an alarm is generated so you can investigate immediately.

What you can monitor

You can monitor

- internal and external telephone numbers (CLIDs) from which you suspect hackers are calling
- mailboxes to which you suspect hackers have gained access
- custom applications that hackers may be using for unauthorized thru-dial activities
- SMTP/VPIM IP addresses, user IDs, and FQDNs

Notification of suspicious activity

You can find out about the alarms generated by

- viewing the Alarms Monitor regularly to learn of new alarms
- setting up an alarm mailbox so that whenever an alarm is generated, the system sends a voice message to the mailbox to alert you
- enabling remote notification or remote text notification for the alarm mailbox so you are notified of new alarm messages immediately at a specified number, such as a pager or cell phone

See also

Chapter 9, “Monitoring suspicious activities,” on page 225

Section C: Mailbox administration

In this section

Overview

Introduction

To manage system resources effectively, you must be able to control resource usage for mailbox class members

When you must re-allocate server resources, you can

- determine how much storage a mailbox is using
- override resource usage controls for an individual mailbox owner

User creation templates and mailbox classes are both used to manage mailbox privileges and properties.

See also

- “Controlling charges incurred by mailbox class members” on page 103
- “Controlling resource usage by mailbox owners” on page 104

User creation templates

Each template provides the default values to be applied to a new group of mailboxes. These values include mailbox capabilities and personal information about mailbox owners such as job title or department.

Once you have used the template to add mailboxes to the CallPilot database, you can override default values for an individual mailbox.

Any changes made to the template have no effect on mailboxes already based on the template.

Mailbox classes

A mailbox class consists of a set of mailbox and messaging privileges that you can assign to mailbox owners. When you update a mailbox class, you automatically update the mailbox privileges of all members of that mailbox class.

See also

- "What mailbox classes govern" on page 102
- "Customizing and configuring mailbox classes" on page 103

A multi-administrator environment

Since mailbox administration of a very large CallPilot system requires much administration time, CallPilot supports delegation of administrative tasks.

Administrators who manage mailbox creation and privileges support administrators who administer mailboxes and mailbox owners.

If you are creating a team of specialized administrators, consider giving responsibility for maintaining user creation templates and mailbox classes to the same administrator.

You can also create administrators to reset passwords only.

See also

- Chapter 1, "CallPilot administration overview," on page 17
- Chapter 4, "Delegating administrative tasks," on page 133

Adding mailboxes

Introduction

Whether you add mailboxes individually or in groups, CallPilot Manager leads you through the steps required to add a single new mailbox owner to the CallPilot database.

You can add new mailboxes with only the following information:

- the name of the user creation template
- first and last names of the mailbox owner
- mailbox number (extension DN)
- *optional:* any shared distribution lists to which the mailbox is to be added

You can also provide information that is common to the group being added at the time of mailbox creation or later.

Using templates to add new mailboxes

CallPilot user creation templates provide a method for you to

- create new mailbox owners efficiently
- document the mailbox properties and user information that were applied to groups of mailbox owners when they were first created

To use this CallPilot feature as it is intended, you must

- maintain a set of user creation templates
- customize the settings for each new group of mailbox owners

You might or might not have to add user creation templates.

Benefits of using templates

When you configure the settings in a template, those settings appear as defaults for any new user mailbox that you create with that template. You can then fill in the user’s name, mailbox number and password, and make changes to the default feature settings if desired.

The template is a starting point for creating the user. If you create a mailbox owner or other user and then reconfigure the template, this does not affect the settings for the already-created user.

Planning a custom set of templates

CallPilot supplies a basic set of user creation templates. When you first configure your CallPilot system, decide which of the supplied templates you need and then customize each to suit your needs.

Adding mailboxes one at a time

If you want to provide all information about a mailbox and its owner at the time you create the mailbox, you must add the mailbox individually.

See “Adding mailboxes, one at a time” on page 293.

Adding a large number of mailboxes at one time

If you must add a large number of mailboxes at one time, use the CallPilot Manager Auto Admin feature. You must use a data input file to specify information that is common to the mailboxes being created (such as language or department). You can update information for an individual mailbox at a later time.

See “Changing individual mailbox properties” on page 301.

See also

- Chapter 13, “Adding and removing mailboxes,” on page 291

- Chapter 14, “Changing mailbox information,” on page 297
- Chapter 17, “Using templates to create new mailboxes,” on page 329

Responding to change requests

Introduction

A mailbox owners can request changes to his or her mailbox configuration under any of the following circumstances:

- The mailbox owner cannot access the mailbox.
- The mailbox owner requests an upgrade in mailbox capacity or functionality.
- The mailbox must be customized to accommodate an atypical scenario.
- The mailbox owner’s personal information has changed.

Correcting access problems

When a mailbox owner cannot access his or her mailbox it might be because of a forgotten password or because the mailbox has been disabled.

If you supervise a team of CallPilot administrators, you might also need to reset CallPilot Manager passwords.

Changing mailbox capabilities

The mailbox class assigned to the user’s mailbox determines the mailbox capabilities.

When a mailbox owner changes job functions, you might need to assign a more appropriate mailbox class to that user.

See “Changing individual mailbox properties” on page 301.

My CallPilot

Mailbox owners can use My CallPilot to reset passwords and update mailbox information.

Customizing a mailbox to accommodate an atypical scenario

You may be asked to configure

- mailboxes to handle fax deliveries and fax machine overflows
- separate mailboxes when the owners share a phoneset
- separate mailboxes when the owners share an extension
- a mailbox for messages for a group with no single phoneset (such as a help desk)
- a mailbox for occasional guests
- a mailbox where callers can leave suggestions
- allowing an assistant to answer a manager’s phoneset when they have separate mailboxes

See “Customizing mailboxes for special purposes” on page 306.

Updating a mailbox owner’s individual information

Mailbox information includes

- the personal information associated with the mailbox
- mailbox storage capacity
- the set of mailbox capabilities (mailbox class)
- the E-mail By Phone voice gender
- the mailbox language
- notification of callers whenever the mailbox owner is using a phoneset extension
- automatic playback of new messages whenever the mailbox is accessed
- notification of new or urgent messages to an external (off-switch) DN

- a change in message waiting indication
- overriding the message blocking defaults set for the associated mailbox class

See “Changing individual mailbox properties” on page 301.

Listing mailboxes that meet specific criteria

Introduction

You must list mailboxes that meet specific criteria whenever you must update mailbox information.

CallPilot provides the following methods for finding mailboxes, mailbox owners, and specialized administrators:

- Find a specific user by name or mailbox number.
- Define a set of search criteria that describes a group of mailboxes, mailbox owners, or administrators.
- Re-use a saved search.

Quick search

When you must find a specific user by name, mailbox number, or department, the quick user search is convenient to use.

Advanced search

When you must find a group of users that satisfies certain search criteria, an advanced search is appropriate.

You can specify a set of up to three search criteria. You base search criteria on information that is stored in the CallPilot database. After you define all search criteria, you can specify whether the search must meet all criteria or any one criterion.

Search criteria

The Search Criteria list provides data elements on which you can base search criteria. To facilitate location of the data type you need, the list is organized into groups that are labeled similarly to groups of settings that can be configured for mailboxes and mailbox classes.

See “Examples of search criteria” on page 289.

Saved searches

Saved searches are available to any administrative user with access to user search functionality.

For efficient administration, an administrator who is comfortable with defining criteria can create, test and save user searches. Then they are available to any specialized administrator with access to user search functionality.

See also

- Chapter 12, “Finding mailboxes, administrators, or directory entries,” on page 281

Managing mailbox privileges

Introduction

A mailbox class consists of a set of mailbox and messaging capabilities that you can assign only to those mailbox owners who need those capabilities.

When you update a mailbox class, you automatically update the mailbox privileges of all mailbox class members.

CallPilot includes supplied mailbox classes to provide you with a starting point to group mailbox owners. You can create custom mailbox classes to suit special needs.

ATTENTION

Plan mailbox classes carefully before you add mailboxes. Re-applying mailbox classes to existing mailbox classes is done individually. It may be more efficient to remove the mailboxes and then use the Auto Admin feature to add them with the new mailbox class specified in the data input file.

What mailbox classes govern

Use mailbox classes to specify the following for mailbox class members:

- mailbox storage capacities and other resource usage controls
- call answering options
- message delivery options
- keycoded features they are permitted to use
- dialing restrictions and permissions for CallPilot messaging features and services that use the thru-dial function

Customizing and configuring mailbox classes

You might need to customize the supplied mailbox classes before you apply them to user creation templates or to individual mailboxes.

To customize a mailbox class, use either of the following methods as they suit your organization’s plans:

- Make basic changes to the supplied template.
- Create new specialized templates by copying the modified basic template and then make specific changes to the specialized templates.

Controlling charges incurred by mailbox class members

Some features and custom applications can place calls to the public network. This means they can incur toll charges.

Since you can assign RPLs to a mailbox class, you can apply different restrictions to different mailbox owner groups. For example, you may allow salespeople who are assigned to one mailbox class to send DTT messages to on-switch and local numbers only, whereas you may allow executives in another class to send DTT messages to certain long-distance area codes.

Recommendations

When you plan RPLs and their application to the features that members of the mailbox class can use, consider

- the calling requirements of the members
- the restrictions necessary for cost management and security of your system

When you modify an RPL, the modifications automatically apply to all features to which the RPL is assigned.

Maintain a change log that identifies each RPL and the features to which it is applied. Use it to date and record all changes to the RPL.

Controlling resource usage by mailbox owners

Use mailbox classes and individual mailbox settings to allocate resources to those mailbox owners who need them most.

When you configure these options, consider the amount of disk space on your system and the basic requirements of the members of the mailbox class.

To control the amount of server space required by each mailbox class member, you can override, for mailbox class members, the following:

- the amount of storage allowed for all messages
- message blocking options
- the length of time that reviewed messages are retained
- message archival capability

Examples

- You can allow your executive mailbox owners or sales mailbox owners to continue to receive messages even if their mailboxes are full.
- You can allow groups of mailbox owners to keep fax messages as long as they keep voice messages, while forcing other groups to delete fax messages sooner.

See also

Chapter 18, “Using mailbox classes to manage mailbox privileges,” on page 339

Section D: Keycoded features and services

In this section

Overview

Introduction

CallPilot provides the following keycoded unified messaging components:

- fax messaging
  See “Fax (multimedia) messaging” on page 111.
- speech-activated messaging
  See “Speech activated messaging” on page 113.
- desktop messaging and My CallPilot
  See “Desktop messaging and My CallPilot” on page 114.
- E-mail By Phone
  See “Email-by-Phone” on page 115.

Use mailbox classes to enable these features for mailboxes.

Availability to customers

CallPilot customers can purchase keycoded unified messaging components: individually when they purchase CallPilot, or they can upgrade the CallPilot server to add one or more keycoded components.

Platform availability

All CallPilot platforms support all unified messaging components.

Networking solutions

Introduction

CallPilot supports the following types of networking solutions:

- VPIM Networking
- Enterprise Networking
- AMIS Networking
- Network Message Service (NMS)

Availability to customers

When you purchase CallPilot Networking, all networking solutions, except for NMS, are available for your site. See “Network Message Service” on page 108.

During installation of CallPilot, you can select the networking solutions you want to install.

VPIM Networking

VPIM Networking provides CallPilot with the capability to exchange multimedia messages over a standard data communications network. Messages can contain voice, fax, or both.

You can use VPIM Networking to network with other CallPilot systems (including CallPilot 150 and BCM), existing Meridian Mail Net Gateway (MMNG) systems, Norstar, or other third-party VPIM-compliant systems.

Enterprise Networking

Enterprise Networking is Nortel Network’s proprietary analog networking protocol for voice messages.

You can use Enterprise Networking to network with other CallPilot systems or existing Meridian Mail systems that support Enterprise Networking.

AMIS-Analog Networking

AMIS-Analog Networking allows users to exchange messages with users of any voice messaging systems that support the AMIS protocol. This protocol is an industry-standard protocol for exchanging voice messages over the telephone line. Its feature set is more limited than those of other networking solutions.

You can use AMIS-Analog Networking to network with other CallPilot systems, existing Meridian Mail systems, Norstar, or other third-party AMIS-compliant systems.

Network Message Service

For Meridian 1 switches and Succession CSE 1000 systems, Network Message Service (NMS) permits one CallPilot messaging server to provide messaging services to users on more than one switch location. In this configuration, a single server connected to one switch can provide services to a number of switches interconnected with the appropriate trunks.

Platform availability

Enterprise, AMIS, and VPIM Networking, and NMS are supported on all CallPilot platforms.

Channel requirements

All AMIS and Enterprise networking solutions require voice channels.

Networking solutions can also use multimedia and speech recognition channels if the resources are available.

VPIM Networking does not require voice channels. Messages are transmitted over the data network.

Limits within networking

Certain limits exist within networking to restrict the number of sites. The following table details these limits:

Item	Limit
Number of private network sites	500
Number of ESN codes	30
Number of CDP steering codes per switch location	500
Number of open VPIM network sites	500
Number of NMS satellite locations	59

See also

Refer to the *CallPilot 1.0 Networking Planning Guide* for detailed information on selecting the type of networking appropriate for your site.

Channel requirements

If a mailbox has fax messaging or speech recognition capability, then fax channels or speech recognition channels are required.

ATTENTION

Each call that is received by a fax-capable mailbox is serviced by a fax channel (the equivalent of two voice channels), regardless of whether or not the caller intends to leave a fax.

Similarly, each call that is received by a speech-capable mailbox is serviced by a speech recognition channel (the equivalent of four voice channels).

Limits

When you plan and configure a CallPilot system with optional unified messaging components, consider imposing the following limits:

- 99 personal distribution lists (PDL), with 200 entries per PDL
- 150 shared distribution lists (SDL), with up to 999 entries per SDL
- maximum number of mailboxes:
  - IPE platform: 8000
  - tower and rackmount platforms: 20 000

Fax (multimedia) messaging

Introduction

A CallPilot mailbox owner can create, send, and receive messages with both voice and fax items only if the mailbox class that is assigned to the mailbox has fax capability enabled.

Creation of messages with both voice and fax items

Messages that contain both voice and fax items can be created in either of the following ways:

- A mailbox owner records a voice annotation for an existing fax message and then forwards the new message.
- A mailbox owner appends a fax message to a voice message via desktop messaging or My CallPilot and sends the new message.

Delivery of messages with both voice and fax items

For messages that contain both voice and fax items, CallPilot assumes that the address is either a telephone number or a fax number.

The items delivered depend on the device that receives the message

IF a message is delivered to a	THEN the result is that
Fax machine	only the fax item is delivered. The message originator receives a non-delivery notification for the voice item of the message.
Answering machine	if an answering machine receives the call and initiates a fax carrier tone at any point during the voice item delivery, the DTT service transfers the message to the DTF service.

IF a message is delivered to a	THEN the result is that
Touch-tone telephone	depends on whether the DTT service is enabled for the mailbox owner and is configured to require DTMF confirmation. ■ If DTMF confirmation is configured, when the recipient indicates DTMF capability (by pressing a key at any point during the DTT session) he or she is prompted to select voice recording or fax delivery, or both. If the recipient has access to a fax machine, he or she can receive the fax or transfer the call to the fax DN. ■ If DTMF confirmation is not configured, the recipient hears the voice item. After the message is delivered and a response is recorded (if there is one), the DTT service transfers the call to the DTF service and attempts fax delivery. If the telephone is a faxphone, the fax item is also delivered. If not, the originator receives a non-delivery notification for the fax item.
Personal computer	if the computer has a voice mail and fax card, both voice and fax items are delivered. If not, the originator receives a non-delivery notification for the fax item.

Channel requirements

If a mailbox has fax messaging capability, then fax channels are required.

ATTENTION

Each call that is received by a fax-capable mailbox is serviced by a fax channel (the equivalent of two voice channels), regardless of whether or not the caller intends to leave a fax.

Speech activated messaging

Introduction

Speech activated messaging is a voice messaging service that is enabled by speech recognition technology. It can be used as an alternative to DTMF commands.

Speech activated messaging enables mailbox owners to speak commands for mailbox navigation, as well as playing, recording, composing and sending messages.

It is particularly useful for

- areas with low DTMF penetration
- mailbox owners who are likely to check their e-mail messages with their hands free (for example, while driving).

Channel requirements

If a mailbox has speech recognition capability, then speech recognition channels are required.

ATTENTION

Each call that is received by a speech-capable mailbox is serviced by a speech recognition channel (the equivalent of four voice channels).

Desktop messaging and My CallPilot

Introduction

Desktop messaging and My CallPilot give mailbox owners access to their CallPilot messages from their PC. Mailbox owners can play back or record voice messages on the PC if it is equipped with a sound card and microphone, or they can choose to use the telephone. Mailbox owners can view fax messages on any PC with a supported Web browser or print them to a fax machine.

Limitations on the number of PCs running the software

There is no limit to the number of PCs that can run the desktop messaging software. There is, however, a limit on the number of mailbox users who can access the Desktop server at one time—a maximum of 1000 concurrent users on a 200i or 201i server, and 5000 concurrent users on a 501t, 702t, 1001rp, or 1002rp server.

LAN requirements

Nortel Networks recommends that you connect the desktop messaging client to the Customer LAN.

Platform availability

Desktop messaging and My CallPilot are supported on the Windows XP, Windows ME, Windows 95, Windows 98, Windows 2000, and Windows NT 4.0 platforms.

See also

For information about engineering Desktop messaging clients, refer to the *CallPilot Desktop Installation Guide* (NTP 555-7101-505).

Email-by-Phone

Introduction

The Email-by-Phone feature enables mailbox owners to listen to e-mail messages over a telephone in much the same way as they listen to voice messages.

See also

“Permitting mailbox class members to listen to e-mail messages over a phoneset” on page 347 and “Configuring and troubleshooting Email-by-Phone” on page 427.

Section E: Custom applications (Application Builder services)

In this section

Application Builder

Introduction

Application Builder is a graphical software program that allows the administrator to create custom applications with both voice and fax functionality that callers can access by dialing telephone numbers.

You can run Application Builder while connected to a CallPilot server, or on its own.

Custom applications

Custom applications typically use voice menus to provide options to callers. A caller experiences an application only through its voice recordings. Callers receive hard-copy information from an application through fax.

To make an application available to callers, add it to the CallPilot SDN Table.

Different levels of Application Builder

CallPilot provides two Application Builder options:

- basic Application Builder, to create applications with voice functionality only
- Application Builder with fax option, to create applications with either or both voice and fax functionality

Availability to customers

Basic Application Builder software is packaged with the CallPilot software and is installed as part of the CallPilot installation on the CallPilot server.

The customer can purchase Application Builder with fax option.

Platform availability

Basic and Application Builder with fax option are supported on all CallPilot platforms.

Channel requirements

Application Builder requires voice channels for voice-supported applications, such as voice menus and announcements.

If Application Builder with fax option is purchased, fax channels must be provisioned.

For more information on calculating the number of voice and fax channels required to support Application Builder, refer to the *CallPilot Planning and Engineering Guide* (NTP 555-7101-101).

Limits within Application Builder

Certain limits exist within Application Builder to restrict the number of items in an application. The following table details these limits:

Item		Limit
Number of Application Builder services **Note:** For the 702t, 100rp, and 100229 rackmount servers, up to 2500 applications can be saved on three volumes.	200i server	500
	201i server	500
	702t, 1001rp, 1002rp servers: Drive D 500 Drive E 100 Drive F 100	2500
Levels of services imported into an Application Builder service		20
Number of faxes stored in an Application Builder service		3000
Number of voice prompts in an Application Builder service		3000

You can install and run Application Builder on more than one personal computer.

Chapter 3

Connecting to the CallPilot server

In this chapter

Logging on to the CallPilot server with CallPilot Manager

Introduction

You must use a web browser to log on to and administer the CallPilot 2.02 server.

ATTENTION

CallPilot Manager can be installed on the CallPilot server or on a stand-alone server. If CallPilot Manager is installed on a stand-alone server, you must know the CallPilot Manager server's host name or IP address, as well as the CallPilot server's host name or IP address.

Logon process

The logon process is completed in two stages:

1. Launch the web browser (on the CallPilot server, or on any PC that has network access to the CallPilot server).

   The web browser on the CallPilot server is configured to automatically connect to the CallPilot Manager web server. If you launch the web browser on a PC, you must specify the URL for the CallPilot Manager web server.

   The URL syntax is http://<*web server host name or IP address*>/cpmgr/.

2. Log on to the CallPilot server with an administrator's mailbox number and password.

   Note: When CallPilot Manager is connected to a CallPilot 2.02 Server from a client, enter the actual CallPilot server name or IP address in the Server box to login. If you enter "local host" instead of the actual CallPilot server name, the administrator cannot connect Application Builder to the

CallPilot server when starting it from CallPilot Manager Web page and calls to telset cannot be made to play or record greetings.

See also

Part 4 of the *CallPilot Installation and Configuration binder*, “Logging on to the CallPilot server with CallPilot Manager.”

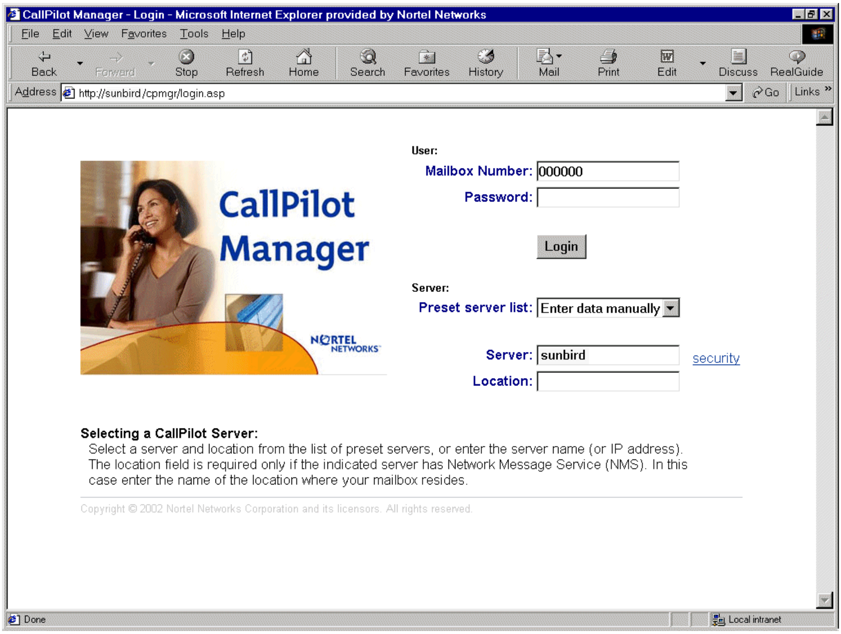
To point the browser to the CallPilot server and log on to CallPilot Manager

1 Launch the web browser on a PC or on the CallPilot server.

2 Type the CallPilot Manager web server’s URL in the Address or Location box of the web browser, and then press Enter.

Example: http://sunbird/cpmgr/

Result: When the connection is established, the CallPilot Manager Logon page appears.



CallPilot Manager - Login - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss RealGuide
Go Links »
CallPilot Manager
NORTEL NETWORKS
Login
security
Done
Local intranet

Address: http://sunbird/cpmgr/login.asp

User:

Mailbox Number: 000000

Password:

Server:

Preset server list: Enter data manually

Server: sunbird

Location:

Selecting a CallPilot Server:

Select a server and location from the list of preset servers, or enter the server name (or IP address). The location field is required only if the indicated server has Network Message Service (NMS). In this case enter the name of the location where your mailbox resides.

Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.

Note: The URL automatically appears as http://<*web server host name or IP address*>/cpmgr/login.asp.

3 Type the administration mailbox number and password.

The supplied administrator mailbox number is **000000**. The default password is **124578**.

4 Do one of the following:

- If connection information has been preconfigured, you can select a server or location from the **Preset server** list box. See “Defining servers and locations for logon” on page 128.
- If Network Message Service (NMS) *is not* installed on the CallPilot server that you are connecting to, type the CallPilot server’s host name or IP address in the **Server** box.
- If Network Message Service (NMS) *is* installed on the CallPilot server that you are connecting to, type the CallPilot server’s host name or IP address in the **Server** box, and then type the name of the switch location on which the administration mailbox resides in the Location box.
- *If you are using Microsoft Internet Explorer:* To reuse information you entered during a prior session on the same PC, do the following:

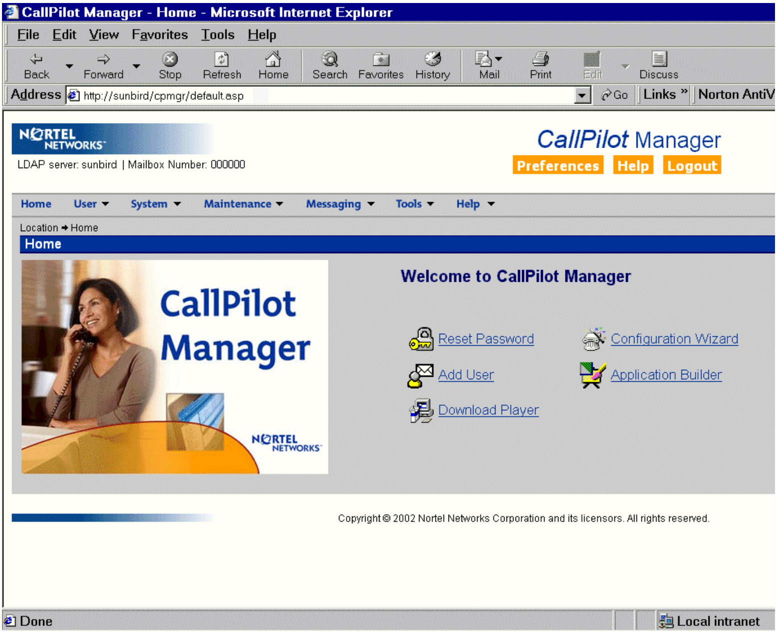
  a.Clear the contents in the box.

  b.Click once inside the box.

  c.Choose the item you need from the list that appears.

5 Click **Login**.

Result: The main CallPilot Manager page appears.


CallPilot Manager - Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://sunbird/cpmgr/default.asp
Go Links Norton AntiV
NORTEL NETWORKS
LDAP server: sunbird | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location → Home
Home
CallPilot Manager
Welcome to CallPilot Manager
Reset Password
Configuration Wizard
Add User
Application Builder
Download Player
Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.
Done
Local intranet

Determining the CallPilot server status

Introduction

Before you can administer the CallPilot server, it must be in operation.

System Ready Indicator

CallPilot Manager displays a System Ready Indicator (SRI) that shows the current status of the CallPilot server. Use the SRI to monitor CallPilot server status at all times and identify problems with CallPilot call processing.

The SRI appears in the upper right corner of each CallPilot Manager web page. The icon indicates the current CallPilot server status. For detailed information about the server status, click the SRI. The status information appears in a separate window.

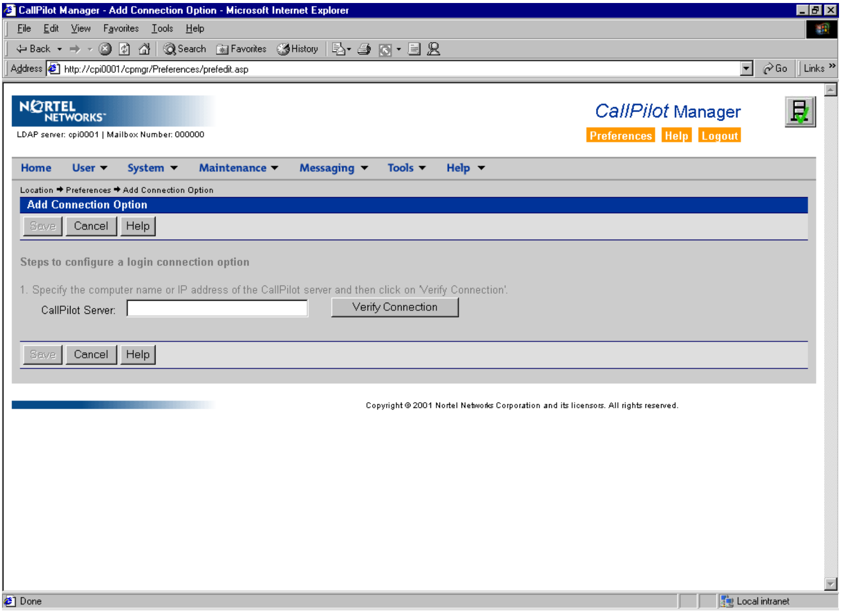
Icon	Status
⌛	Starting - CallPilot server is starting up.
✓	Ready - CallPilot server is in full operation.
⚠	Warning - Calls are being processed but some accompanying services are not functioning.
✖	Failure - Calls are not being processed.
?	Unknown - Status information about the CallPilot server is currently unavailable.

Defining servers and locations for logon

Introduction

If CallPilot administrators are responsible for more than one CallPilot server, use CallPilot Manager to configure any CallPilot server in your messaging system. Define the connection settings for the CallPilot servers in your messaging system so that administrators can quickly select a server and NMS location when they log on to CallPilot Manager. You can add or remove specific servers as required.

Getting there: Preferences → Preferences page → List of logon shortcuts for this web server



CallPilot Manager - Add Connection Option - Microsoft Internet Explorer

Address http://cpi0001/cpmgr/Preferences/prefedit.asp

LDAP server: cpi0001 | Mailbox Number: 000000

Location → Preferences → Add Connection Option

Add Connection Option

Steps to configure a login connection option

1. Specify the computer name or IP address of the CallPilot server and then click on 'Verify Connection'.

CallPilot Server:

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

Looking up procedures in CallPilot Manager online Help

To display a relevant Help topic, click the Help button on the page. Look up procedures for adding and removing servers and locations by opening the **Delegating administrative tasks** book in the Help Contents.

Setting security options for CallPilot Manager sessions

Introduction

You can enable Secure Socket Layer (SSL) to encrypt data transmissions between the CallPilot Manager client and the CallPilot web server. You can set default security options for servers defined in the CallPilot Manager Preferences, and specify whether these defaults always apply to other CallPilot servers you configure with CallPilot Manager.

ATTENTION SSL requires additional bandwidth. Consider the available bandwidth and CallPilot Manager traffic in your system when you decide which SSL option to use.

SSL options

SSL must be enabled both on the web server and in the client web browser to secure communications

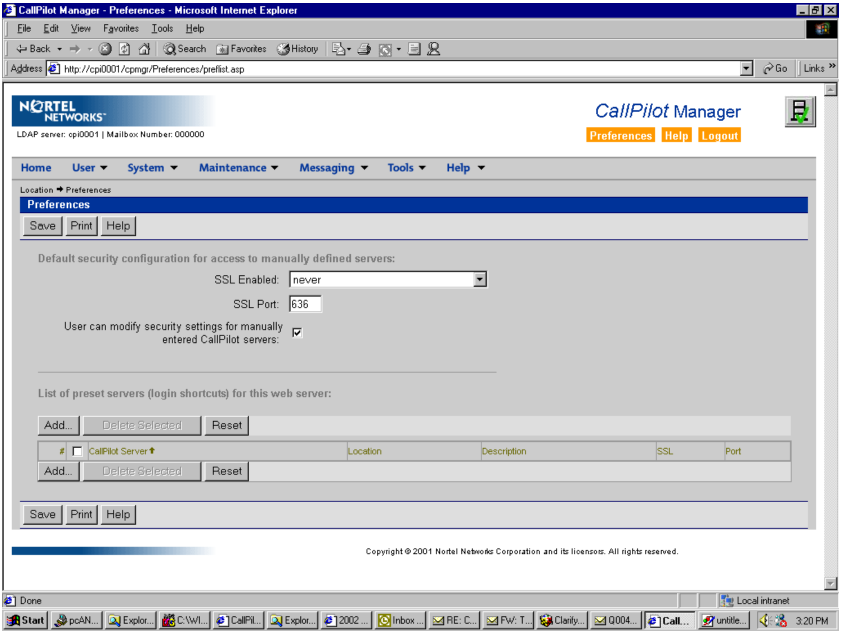
Option	Result
Never	No data transmissions are encrypted.
For the entire session	All data transmissions are encrypted until you log out of CallPilot Manager.
Only for logon and password changes	Only mailbox and password data transmissions are encrypted.

Allowing other administrators to modify security options

You can do either of the following:

- Allow administrators to select security options for undefined servers at logon
- Always apply the default security options to pre-defined or manually specified server.

Getting there: Preferences → Preferences page


CallPilot Manager - Preferences - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location ➜ Preferences
Preferences
Save Print Help
Add... Delete Selected Reset
Done
Local intranet
Start pcAN... Explor... C:\WI... CallPil... Explor... 2002 ... Inbox ... RE: C... FW: T... Clarify... Q004... Call... untitle... 3:20 PM

Address http://cpi0001/cpmgr/Preferences/preflist.asp

LDAP server: cpi0001 | Mailbox Number: 000000

Default security configuration for access to manually defined servers:

SSL Enabled: never

SSL Port: 636

User can modify security settings for manually entered CallPilot servers: ☑

List of preset servers (login shortcuts) for this web server:

#	☐	CallPilot Server	Location	Description	SSL	Port

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

Looking up procedures in CallPilot Manager online Help

Look up the procedure for setting security options by opening the **Getting Started** book in the Help Contents.

Chapter 4

Delegating administrative tasks

In this chapter

Overview

Introduction

CallPilot Manager provides the functionality to perform diverse administrative tasks.

The administrators who use CallPilot Manager can be distributors, support technicians, or customer staff administrators.

If you are an administrator with all rights, you can

- Create and maintain a set of user creation templates and mailbox classes to support management of a group of CallPilot administrators.
- Set up support technicians as “administrators without mailboxes” with all administration rights.
- Assign specific administrative privileges to mailbox owners to whom certain tasks can be delegated. These administrators are referred to as *specialized administrators*.
- Assign all administrative rights to mailbox owners. These administrators are referred to as *global administrators*.

Using templates to add administrators

If you are maintaining a staff of specialized administrators

- Create a set of user creation templates (based on one of the supplied administrator templates).
- Add a group of administrators in a single operation.
- Update the administrative staff by adding administrators, one at a time.

Supplied administrator templates

- Admin Only Template (see “Admin Only Template” on page 136)
- Administrator Template (see “Administrator Template” on page 138)

See also

- “About CallPilot administration” on page 31
- “Adding full administrators without mailboxes” on page 136
- “Adding mailbox owners with some administrative privileges” on page 138
- “Assigning and suspending administrative privileges” on page 142
- “Creating specialized administrators” on page 144
- Chapter 17, “Using templates to create new mailboxes,” on page 329
- Chapter 18, “Using mailbox classes to manage mailbox privileges,” on page 339

Adding full administrators without mailboxes

Introduction

Use the Admin Only Template to add a group of administrators who have access to all CallPilot Manager administrative functions, but do not have mailbox privileges.

Admin Only Template

The Admin Only Template has the following defaults defined:

Setting	Default value
Administration Type	Full User Without Mailbox
Mailbox Class	Administrator
DTT DTMF confirmation required	Enabled
Auto deletion of invalid PDL addresses	Enabled

Information you need

- the name of the user creation template that provides information for the administrator type (based on the Admin Only Template)
- first and last names of the CallPilot administrators
- *If you are adding a group of administrators:*
  - the name and path of the formatted data input file that contains new administrator information
  - *If the input data file is an Excel spreadsheet:* the name of the worksheet on which the data is stored

See also

- “Overview” on page 134
- “Adding an individual administrator” on page 140
- “Adding a group of administrators” on page 141
- Chapter 17, “Using templates to create new mailboxes,” on page 329
- Chapter 18, “Using mailbox classes to manage mailbox privileges,” on page 339

Adding mailbox owners with some administrative privileges

Introduction

Use the Administrator Template to add mailbox owners with the same access to CallPilot Manager functionality.

Administrator Template

The Administrator Template has the following defaults defined:

Setting	Default value
Administration Type	Mailbox owner with some administrative privileges
Mailbox Class	Administrator
Block incoming messages	Never
DTT DTMF confirmation required	Enabled
Auto deletion of invalid PDL addresses	Enabled

Information you need

- the name of the user creation template that provides information for the administrator type (based on the Administrator Template)
- first and last names of the CallPilot administrator
- the set of administrative rights required by the administrator
- mailbox number (extension DN)
- *optional:* shared distribution lists to which the administrator must be added

- *If you are adding a group of administrators:*
  - the name and path of the formatted data input file that contains new administrator information
  - *if the input data file is an Excel spreadsheet:* the name of the worksheet on which the data is stored

See also

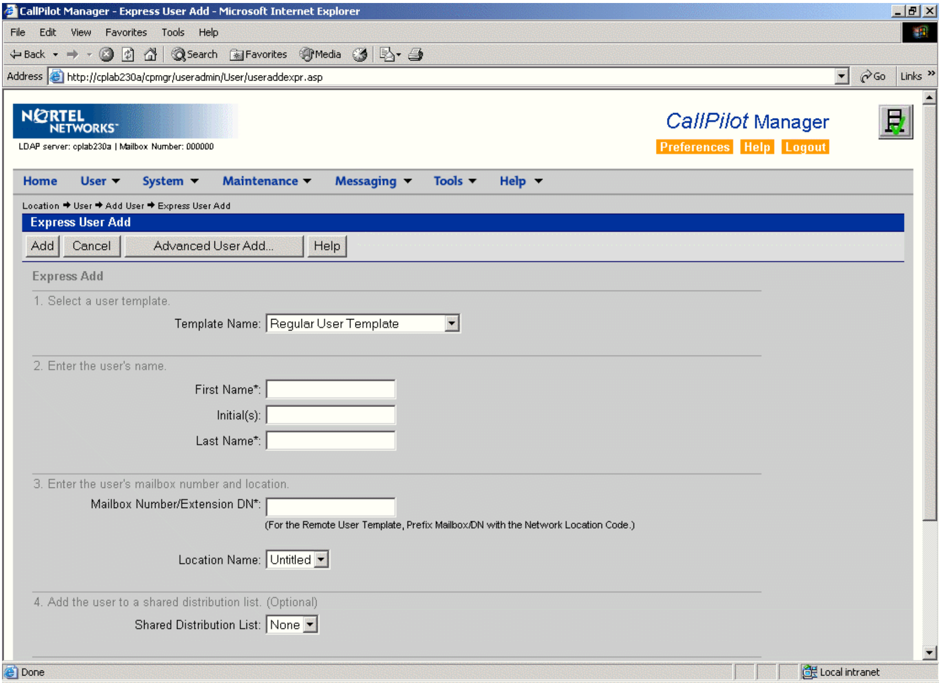
- “Overview” on page 134
- “Adding an individual administrator” on page 140
- “Adding a group of administrators” on page 141
- “Creating specialized administrators” on page 144
- Chapter 17, “Using templates to create new mailboxes,” on page 329
- Chapter 18, “Using mailbox classes to manage mailbox privileges,” on page 339

Adding an individual administrator

Introduction

To add administrators one at a time, use the same feature that you use to add mailboxes one at a time: Express User Add. Use a template based on either the supplied Admin Only Template or the Administrator Template.

Getting there: User → Add User → Express User Add page


CallPilot Manager - Express User Add - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://cplab230a/cpmgr/useradmin/User/useraddexpr.asp
Go Links
NORTEL NETWORKS
LDAP server: cplab230a | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location → User → Add User → Express User Add
Express User Add
Add Cancel Advanced User Add... Help
Express Add
Done
Local intranet

1. Select a user template.

Template Name: Regular User Template

2. Enter the user's name.

First Name*:

Initial(s):

Last Name*:

3. Enter the user's mailbox number and location.

Mailbox Number/Extension DN*:

(For the Remote User Template, Prefix Mailbox/DN with the Network Location Code.)

Location Name: Untitled

4. Add the user to a shared distribution list. (Optional)

Shared Distribution List: None

Looking up procedures in CallPilot Manager online Help

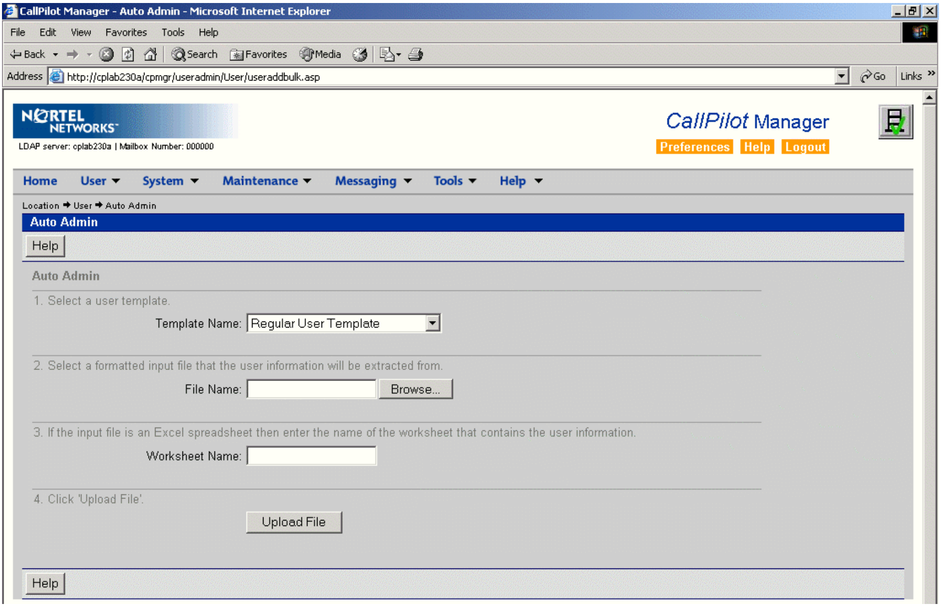
In the CallPilot Manager online Help, locate procedures for adding and removing administrators by looking up **administrators** in the Index.

Adding a group of administrators

Introduction

To add a group of administrators in a single operation, use the same feature that you use to add a group of mailboxes: Auto Admin feature. Use a template based on either the supplied Admin Only Template or the Administrator Template.

Getting there: User → Auto Admin


CallPilot Manager - Auto Admin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://cplab230a/cpmgr/useradmin/User/useraddbulk.asp
Go Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help

LDAP server: cplab230a | Mailbox Number: 000000

Location → User → Auto Admin

Auto Admin

Help

Auto Admin

1. Select a user template.

Template Name: Regular User Template

2. Select a formatted input file that the user information will be extracted from.

File Name: Browse...

3. If the input file is an Excel spreadsheet then enter the name of the worksheet that contains the user information.

Worksheet Name:

4. Click 'Upload File'.

Upload File

Help

Looking up procedures in CallPilot Manager online Help

In the CallPilot Manager online Help, locate procedures for adding and removing administrators by looking up **administrators** in the Index.

Assigning and suspending administrative privileges

Introduction

You can assign administrative privileges to an existing mailbox owner and suspend the administrative privileges of an existing administrator.

Assigning administrative privileges

To assign administrative privileges to an existing mailbox owner, display the mailbox owner’s user properties and, in the Administrative Rights box, click “User with some administrative rights.”

After you have determined the tasks to be performed by the mailbox owner, you can grant only those administrative privileges required to carry out the required tasks.

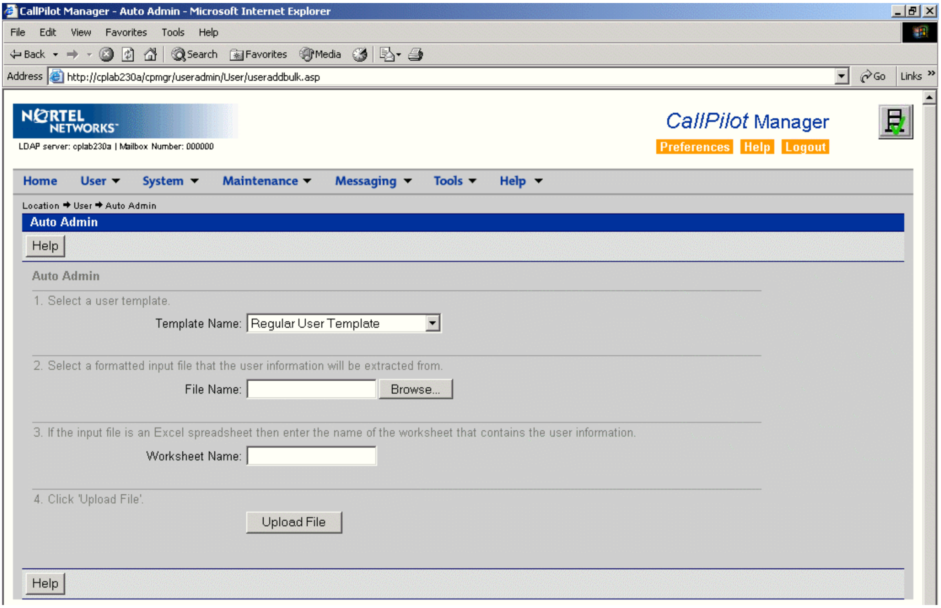
Suspending administrative privileges

Once you have assigned administrative privileges to a support technician or mailbox owner, you can suspend them temporarily if, for example, the administrator takes a leave of absence and is expected to resume administrative responsibilities.

See also

- “About CallPilot administration” on page 31
- “Overview” on page 134
- “Creating specialized administrators” on page 144

Getting there: User → User Search → User Properties sheet



CallPilot Manager - Auto Admin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://cplab230a/cpmgr/useradmin/User/useraddbulk.asp
Go Links
NORTEL NETWORKS
LDAP server: cplab230a | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location ➔ User ➔ Auto Admin
Auto Admin
Help

Auto Admin

1. Select a user template.

Template Name: Regular User Template

2. Select a formatted input file that the user information will be extracted from.

File Name:

3. If the input file is an Excel spreadsheet then enter the name of the worksheet that contains the user information.

Worksheet Name:

4. Click 'Upload File'.

Looking up procedures in CallPilot Manager online Help

Look up procedures for assigning and suspending administrative privileges by looking up **administrative privileges** in the Index.

Creating specialized administrators

Introduction

If you are administering a CallPilot system with thousands of mailboxes, you might delegate some of your tasks to specialized administrators. Typically, a specialized administrator is located at the customer site and performs ongoing maintenance such as resetting mailbox passwords and changing mailbox owner information.

A specialized administrator is a mailbox owner who has been granted access to specified CallPilot Manager functions.

Information you need

- the tasks that will be assigned to the mailbox owner
- the set of administrative rights required by the administrator

Limitation

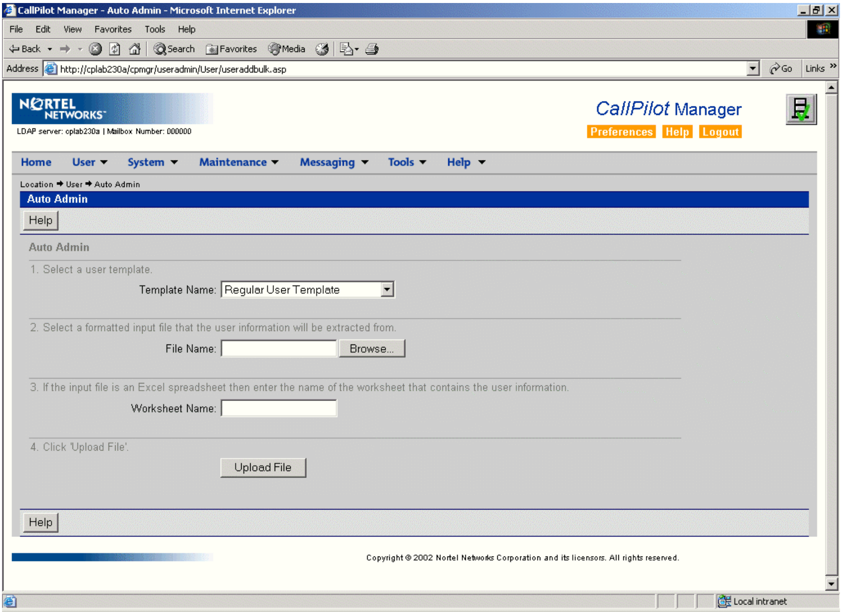
You cannot assign administrative privileges to a mailbox owner on a remote server.

Supporting specialized administrators

If you are maintaining a staff of specialized administrators and support more than one CallPilot server or location, define all servers and locations to facilitate logon by administrators. See “Defining servers and locations for logon” on page 128.

Administrator Template

You can set up specialized administrators with any combination of CallPilot administrative privileges.



CallPilot Manager - Auto Admin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://cplab230a/cpmgr/useradmin/User/useraddbulk.asp
Go Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Local intranet

LDAP server: cplab230a | Mailbox Number: 000000

Location → User → Auto Admin

Auto Admin

Help

Auto Admin

1. Select a user template.

Template Name: Regular User Template

2. Select a formatted input file that the user information will be extracted from.

File Name: Browse...

3. If the input file is an Excel spreadsheet then enter the name of the worksheet that contains the user information.

Worksheet Name:

4. Click 'Upload File'.

Upload File

Help

Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.

Looking up procedures in CallPilot Manager online Help

Look up procedures for assigning and suspending administrative privileges by looking up **administrative privileges** in the Index.

Examples of specialized administrators you can create

The examples in this section are based on the list of administrative privileges found in the Administrator Template.

Example 1: Mailbox maintenance administrator

Mailbox Maintenance administrators can reset mailbox passwords, add mailbox owners, delete mailbox owners, and update mailbox information. Classify these administrators as “users with some administration rights” with any of all of the following:

- User Administration rights
- Shared Distribution List (SDL) Administration rights
- Backup/Restore Administration rights (to maintain and use user archives)
- *If desktop messaging and My CallPilot are installed:* My CallPilot Administration rights

Example 2: Mailbox Privileges administrator

Mailbox Privileges administrators maintain mailbox classes to control access to CallPilot resources. Classify these administrators as “users with some administration rights” with any or all of the following:

- Mailbox Class Administration rights only
- User Administration rights (to enable maintenance of user creation templates)
- Restriction Permission List Administration rights (to create specialized RPLs)

Example 3: Mailbox Security administrator

Mailbox Security administrators configure mailbox access controls for all mailboxes. Classify these administrators as “users with some administration rights” with

- Security Administration rights
- User Administration rights (to confirm use of personal verifications)
- Restriction Permission List Administration rights (to create specialized RPLs)

Example 4: Messaging Configuration administrator

Messaging Configuration administrators specify the message delivery rules for the entire CallPilot system. Classify these administrators as “users with some administration rights” with the following:

- Message Delivery Configuration Administration rights
- Messaging Administration rights
- Dialing Information Administration rights
- Holidays Administration rights
- *If delivery to non-mailbox DNs is permitted:* Outcalling Administration rights
- Restriction Permission List Administration rights (to create specialized RPLs)

Example 5: Mailbox Service administrator

Messaging Service administrators add and configure CallPilot services such as fax and fax broadcast services, speech activated messaging services, and E-mail by Phone service. Classify these administrators as “users with some administration rights” with the following:

- Server Settings Administration rights
- Backup/Restore Administration rights (to maintain and use prompt archives and application archives)
- Service Directory Number Administration rights
- Message Network Configuration Administration rights
- Internet Mail Clients Administration rights
- External E-mail Server Administration rights
- *If delivery to non-mailbox DNs is permitted:* Outcalling Administration rights
- Restriction Permission List Administration rights
- System Prompt Customization Administration rights
- Application Builder Administration rights (to set up voice menus and other custom applications)

Chapter 5

Configuring dial-up access to the CallPilot server

In this chapter

Overview

Remote control of the server

You can control the CallPilot server as though you were sitting at a keyboard connected directly to it from a personal computer that is connected to the server in either of the following ways:

- over a dial-up connection
- over a LAN connection

Remote tasks

Once you have established the pcAnywhere session, you can take direct control of the CallPilot server to

- query the server event logs
- use Windows System Tools to maintain the CallPilot server
- apply PEPs

Requirements

- The pcAnywhere host must be working on the CallPilot server.
- If the server is powered off, you cannot establish a connection with the server. Someone at the server’s location must start the server. The pcAnywhere host is automatically launched when the server is started.

Task summary

The tasks you perform depends on whether the remote personal computer is connected to the CallPilot server over a LAN or a dial-up connection.

Task	For a LAN connection?	For a dial-up connection?
1 “Installing the pcAnywhere client on the remote personal computer” on page 156	Yes	Yes
2 “Configuring the pcAnywhere client for dial-up to the CallPilot server” on page 157	Yes	Yes
3 “Creating the Dial-Up Networking connection profile” on page 163	No	Yes
4 “Establishing a connection using Dial-Up Networking” on page 168	No	Yes
5 “Taking remote control of the CallPilot server” on page 173	Yes	Yes
6 “Optimizing remote host response during a pcAnywhere session” on page 174	No	Yes
7 “Ending a dial-up connection” on page 176	No	Yes

Testing a LAN connection

If the personal computer and the CallPilot server are on the same LAN, you do not need to establish a dial-up connection. A LAN connection may be set up between the personal computer and the CallPilot server’s CLAN or ELAN card.

To test the LAN connection, ping the IP address of the CLAN or ELAN card on the server. If the server does not respond, check the cabling and the remote personal computer’s TCP/IP configuration information.

Section A: Configuring pcAnywhere on a personal computer

In this section

About pcAnywhere

Introduction

One licensed copy of the pcAnywhere 10.5 host is installed on the CallPilot server at the factory. This allows the CallPilot server operator to accept control of the server by an operator at a remote personal computer with the pcAnywhere 10.5 client installed on it.

Administrators can use pcAnywhere over a dial-up, direct cable, or network connection to

- query server event logs
- shut down and restart the server
- perform limited file transfers between the personal computer and the CallPilot server
- start CallPilot Manager and use it to monitor the system and perform administration tasks
- use local Windows System Tools to maintain the CallPilot server

Requirement

You must purchase a license from the vendor for installation of pcAnywhere on any personal computer used for remote administration of a CallPilot server.

pcAnywhere security features

- a host assessment tool for analyzing the security of your remote access
- logging of unauthorized access attempts

When you start pcAnywhere for the first time

1 Start **Symantec pcAnywhere**.

Result: The Smart Setup Wizard window appears.

2 Click Next.

Result: The Network Device window appears.

3 Ensure that **TCP/IP** is selected as the network device and then click Next.

4 Click **Finish**.

5 Change the **Host Operation video mode** from the default setting to **Compatibility.** For instructions, refer to the pcAnywhere online help.

Installing the pcAnywhere client on the remote personal computer

Introduction

Nortel Networks does not provide additional licenses for installing pcAnywhere on remote personal computers. You must purchase a license from the vendor for installation of pcAnywhere on any personal computer used for remote administration of a CallPilot server.

To install software on the personal computer, you must be logged on as an administrator.

Hardware changes and pcAnywhere

If you need to change the video driver on the remote personal computer, you must first uninstall pcAnywhere.

See also

For specific instructions on installing the pcAnywhere client, refer to the Symantec pcAnywhere documentation.

Configuring the pcAnywhere client for dial-up to the CallPilot server

Introduction

To connect to the CallPilot server, first create a pcAnywhere remote control connection to the server.

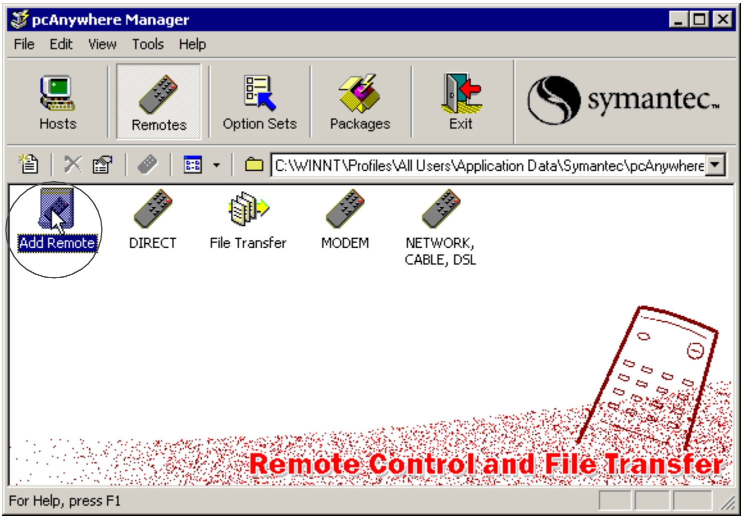
See also

For specific instructions on configuring the pcAnywhere client, refer to the Symantec pcAnywhere documentation.

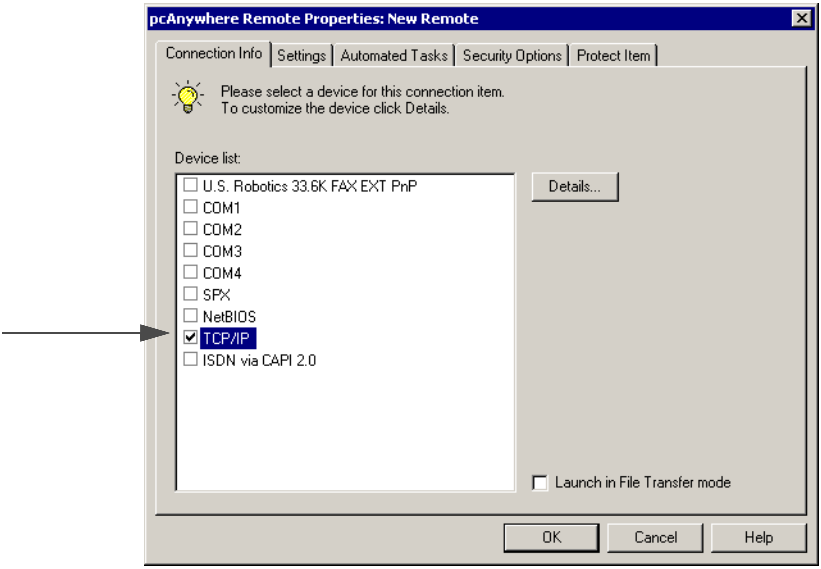
Entering the required settings

The following illustrations show you the settings that you must enter to configure the pcAnywhere connection from the remote personal computer to the CallPilot server.

1. Use pcAnywhere Manager to configure the remote properties of the CallPilot server connection:



2. On the Connection Info page, configure the connection to use TCP/IP:


pcAnywhere Remote Properties: New Remote

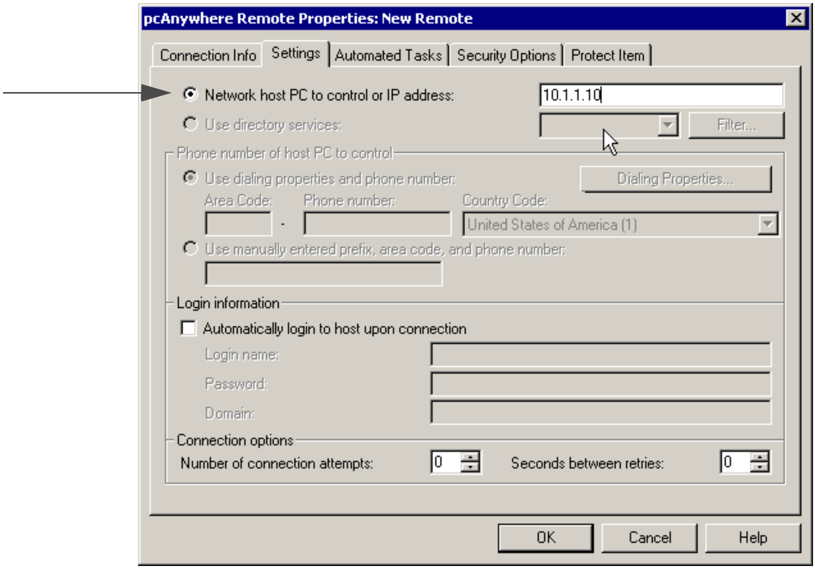
Please select a device for this connection item.
To customize the device click Details.

Device list:

- ☐ U.S. Robotics 33.6K FAX EXT PnP
- ☐ COM1
- ☐ COM2
- ☐ COM3
- ☐ COM4
- ☐ SPX
- ☐ NetBIOS
- ☑ TCP/IP
- ☐ ISDN via CAPI 2.0

☐ Launch in File Transfer mode

3. On the Settings page, identify the CallPilot server as the host:



pcAnywhere Remote Properties: New Remote

● Network host PC to control or IP address: 10.1.1.10

○ Use directory services:

Phone number of host PC to control

● Use dialing properties and phone number:

Area Code: Phone number: Country Code: United States of America (1)

○ Use manually entered prefix, area code, and phone number:

Login information

□ Automatically login to host upon connection

Login name:

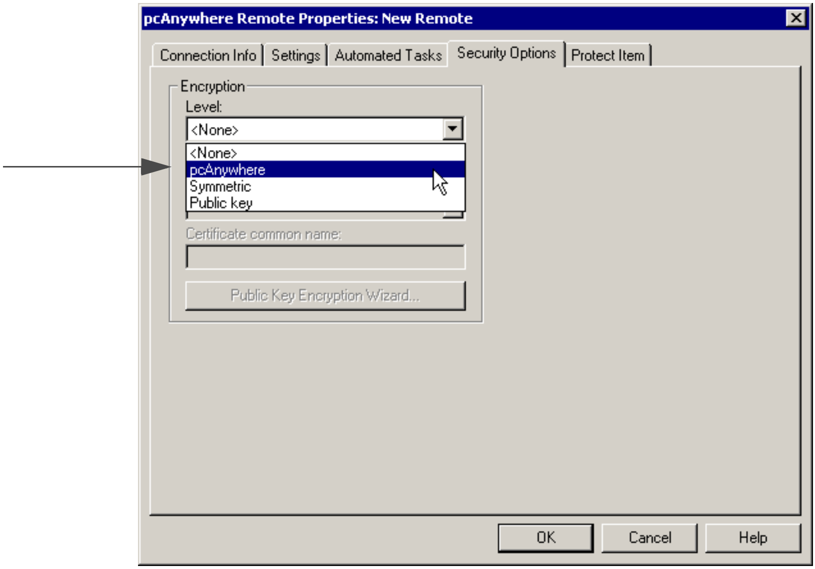
Password:

Domain:

Connection options

Number of connection attempts: 0 Seconds between retries: 0

4. On the Security Options page, select the encryption level:



pcAnywhere Remote Properties: New Remote

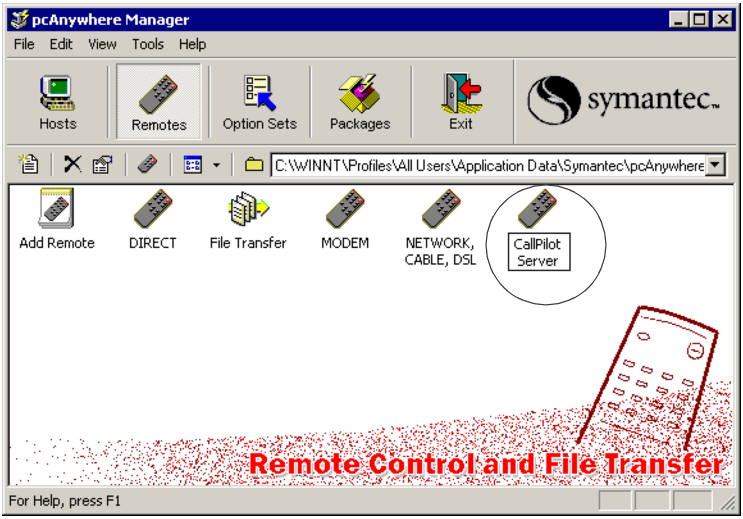
Encryption

Level: <None>

Certificate common name:

5. Click OK to add the new connection icon to the pcAnywhere Manager window.

6. Name the connection:



What’s next?

If you are using pcAnywhere on a remote personal computer, continue with Section B: “Establishing a dial-up connection to the server,” on page 161.

If you are using pcAnywhere on a personal computer that is on the same LAN as the CallPilot server, continue with “Taking remote control of the CallPilot server,” on page 173.

Section B: Establishing a dial-up connection to the server

In this section

Dial-Up Networking

Introduction

A dial-up connection enables you to establish a connection between the CallPilot server and a personal computer over the public switch telephone network (PSTN).

Once you have established a dial-up connection, it appears as if the CallPilot server and the personal computer are on the same LAN.

You can use a dial-up connection to

- perform limited file transfers between the personal computer and the CallPilot server
- point your browser to CallPilot Manager
- use Windows System Tools to maintain the CallPilot server

Required software

To connect to the CallPilot server from a personal computer that is not to the same LAN, you must use Windows Dial-Up Networking and Remote Access Service (RAS) software.

Note: To administer the CallPilot server from a remote personal computer, you can use pcAnywhere software.

Dial-Up Networking software is usually installed during the installation of the operating system. If the Dial-Up Networking folder does not appear in the My Computer window, the software is not installed. Refer to your Windows documentation for a Dial-Up Networking installation procedure.

Remote Access Service (RAS) and pcAnywhere 10.5 are installed on the CallPilot server at the factory. No on-site configuration is required.

Creating the Dial-Up Networking connection profile

Introduction

The Windows Dial-Up Networking software enables you to establish a connection between the server and the remote personal computer over the publish switch telephone network (PSTN). This is not required for personal computers that are on the same LAN as the server.

Note: If the My Computer folder does not contain the Dial-Up Networking folder, the Dial-Up Networking software has not been installed. Refer to your Windows documentation for an installation procedure.

When a connection profile is created, an icon representing the connection profile appears in the Dial-Up Networking folder.

Information you need

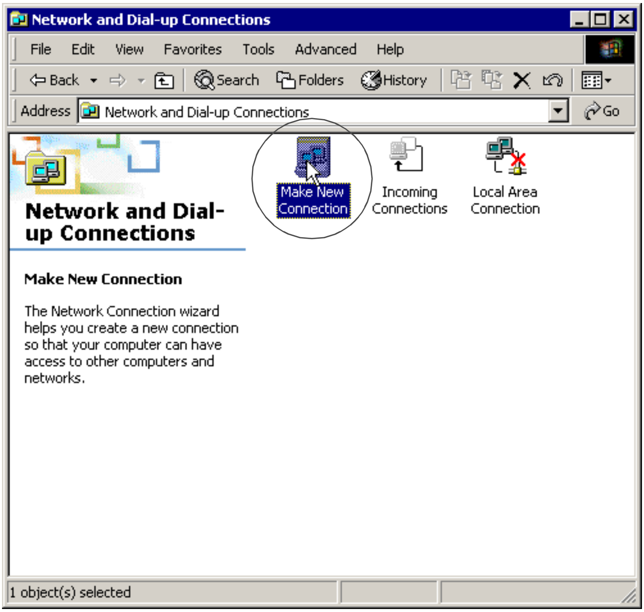
If you do not know the following information, contact the system administrator:

- the server telephone number
- the server IP address

To create a dial-up connection profile for a CallPilot server

Note: The following illustrations were created on a personal computer running Windows 2000. When you create a dial-up connection profile on a computer running a different Windows operating system, the wizard may be accessed and presented differently.

1 Log on to the remote personal computer and start the Make New Connection wizard.

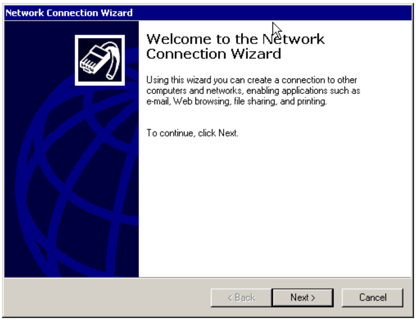

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
Make New Connection
Incoming Connections
Local Area Connection

Make New Connection

The Network Connection wizard helps you create a new connection so that your computer can have access to other computers and networks.

1 object(s) selected

Result: The Network Connection Welcome appears.



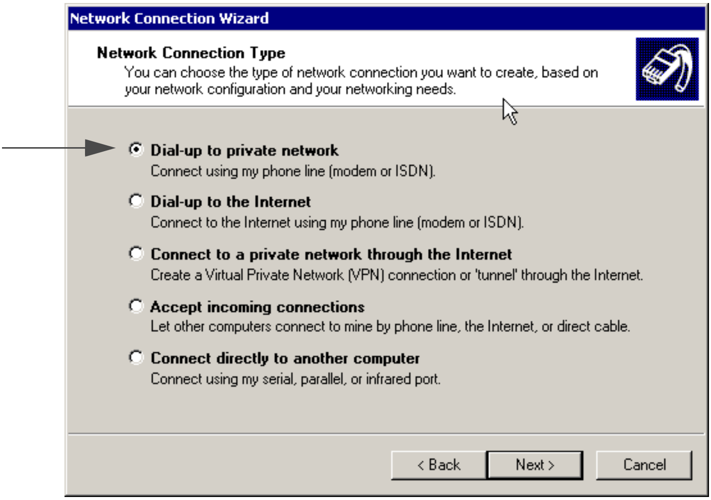
Welcome to the Network Connection Wizard

Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.

To continue, click Next.

2 Click **Next**.

3 Define the Network Connection Type as **Dial-up to private network**, then click **Next**.



Network Connection Wizard

Network Connection Type

You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

● **Dial-up to private network**
Connect using my phone line (modem or ISDN).

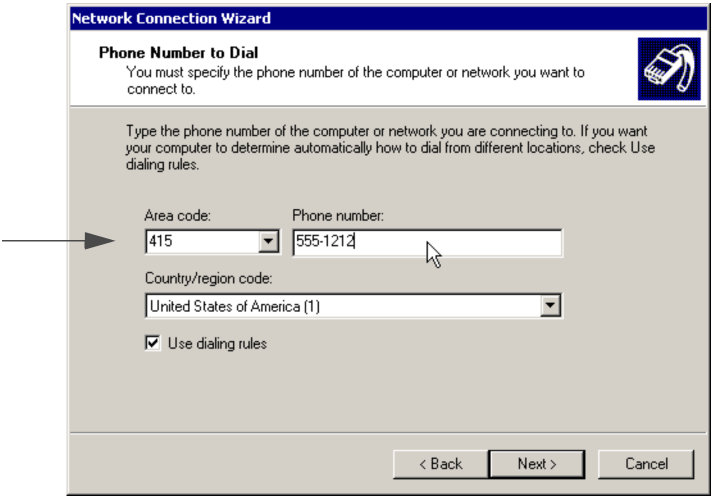
○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

○ **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

4 Enter the server telephone number, then click **Next**.



Network Connection Wizard

Phone Number to Dial

You must specify the phone number of the computer or network you want to connect to.

Type the phone number of the computer or network you are connecting to. If you want your computer to determine automatically how to dial from different locations, check Use dialing rules.

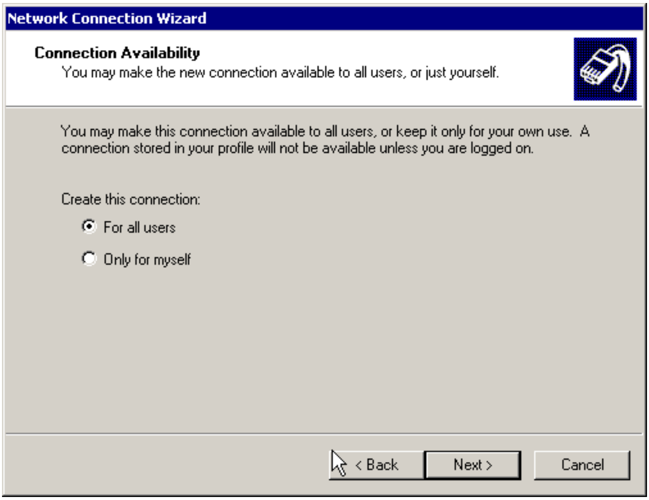
Area code: 415

Phone number: 555-1212

Country/region code: United States of America (1)

☑ Use dialing rules

5 Specify the connection availability (for all users or only for the CallPilot administrator), then click **Next**.



Network Connection Wizard

Connection Availability
You may make the new connection available to all users, or just yourself.

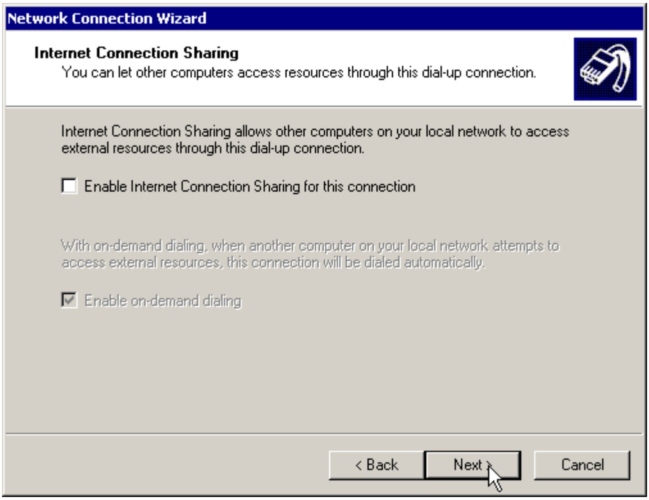
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:

● For all users

○ Only for myself

6 When prompted to allow Internet Connection Sharing, click **Next**.



Network Connection Wizard

Internet Connection Sharing
You can let other computers access resources through this dial-up connection.

Internet Connection Sharing allows other computers on your local network to access external resources through this dial-up connection.

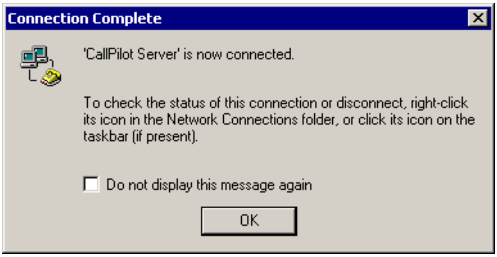
□ Enable Internet Connection Sharing for this connection

With on-demand dialing, when another computer on your local network attempts to access external resources, this connection will be dialed automatically.

☑ Enable on-demand dialing

7 Type the name you want to use for the connection, then click **Finish**.

Result: The following confirmation message appears.



Connection Complete

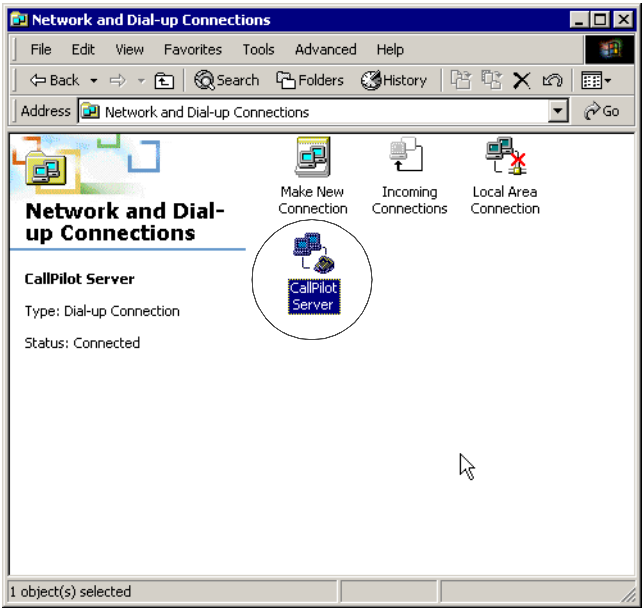
'CallPilot Server' is now connected.

To check the status of this connection or disconnect, right-click its icon in the Network Connections folder, or click its icon on the taskbar (if present).

□ Do not display this message again

Click **OK**.

Result: The dial-up connection icon for the CallPilot server appears in the Network and Dial-up Connections window.



Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Incoming Connections
Local Area Connection
CallPilot Server

Network and Dial-up Connections

CallPilot Server

Type: Dial-up Connection

Status: Connected

1 object(s) selected

Establishing a connection using Dial-Up Networking

Introduction

To perform remote administration of a CallPilot server from a personal computer that is not located on the same LAN as the server, you must establish a Dial-Up Networking connection between the personal computer and the server.

If the personal computer and the CallPilot server are on the same LAN, the procedures in this section are not required.

Before you begin

- Ensure that you have created a server connection profile. See “Creating the Dial-Up Networking connection profile” on page 163.
- A user ID and password to log on to the customer’s network. Obtain this information from the customer.
- If you are using pcAnywhere, you need the password for a remote access user account (for example, the NGenDist user account) and pcAnywhere caller account on the server (for example, the NGenDist caller account).

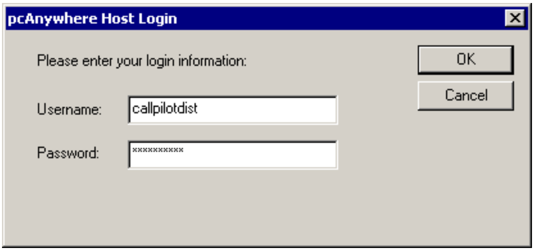
To establish a dial-up connection to the CallPilot server

1 Log on to the remote personal computer and start **Network and Dial-Up Connections**.

2 Double-click the CallPilot server icon.

Note: If the icon is unavailable, you have not created a server connection profile. See “Creating the Dial-Up Networking connection profile” on page 163.

3 If prompted for a user ID and password, enter the use ID and password to log on to the customer’s network.



pcAnywhere Host Login

Please enter your login information:

Username: callpilotdist

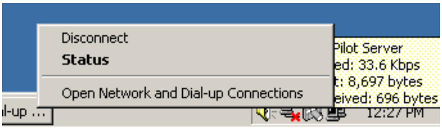
Password: ***********

4 Wait until the connection is established.

To display status details about the CallPilot server

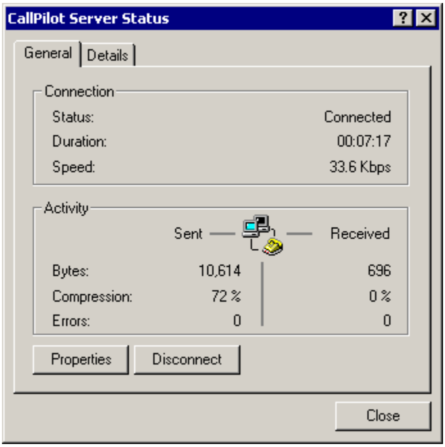
1 Right-click the icon on the toolbar.

Result: A menu appears.



2 Click **Status**.

Result:



CallPilot Server Status

General | Details

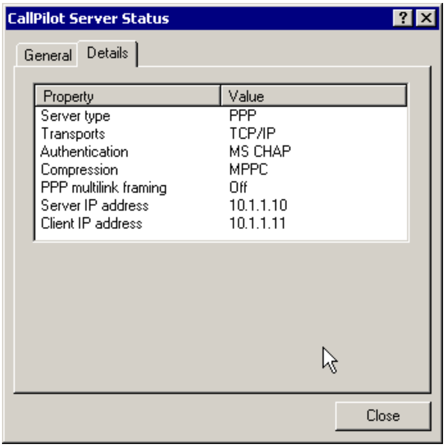
Connection

Status:	Connected
Duration:	00:07:17
Speed:	33.6 Kbps

Activity

	Sent	Received
Bytes:	10,614	696
Compression:	72 %	0 %
Errors:	0	0

3 Click the **Details** tab.



CallPilot Server Status

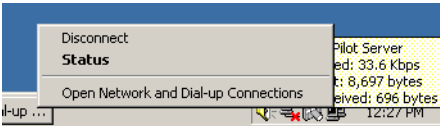
General | Details

Property	Value
Server type	PPP
Transports	TCP/IP
Authentication	MS CHAP
Compression	MPPC
PPP multilink framing	Off
Server IP address	10.1.1.10
Client IP address	10.1.1.11

To reconfigure a dial-up connection profile

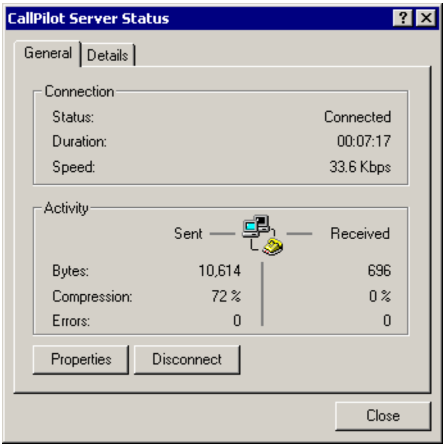
1. Right-click the icon on the toolbar.

   Result: A menu appears.



2. Click **Status**.

   Result:



CallPilot Server Status

General | Details

Connection

Status: Connected

Duration: 00:07:17

Speed: 33.6 Kbps

Activity

	Sent	Received
Bytes:	10,614	696
Compression:	72 %	0 %
Errors:	0	0

3. Click **Properties**.
4. Enter the telephone number of the server if it is not already present or if it is incorrect. Make any other required changes.
5. Click **Configure**.
6. Click **OK**.
7. Click the **Server Settings** tab.
8. For Dial-Up Server, select **PPP**.
9. For the network protocols, select only **TCP/IP** and **NETBEUI**.
10. Click the **TCP/IP** settings tab.

11 Select **Specify an IP address**, and enter the server IP address.

12 Select **Use default gateway on remote network**.

13 The remaining fields are optional. Fill them in as required for the customer’s network.

14 Click **OK**.

What’s next?

After the connection has been made, you can do the following tasks:

- Start CallPilot Manager. See “Logging on to the CallPilot server with CallPilot Manager” on page 122.
- Use pcAnywhere to control the server as you perform administrative tasks. See “Taking remote control of the CallPilot server,” on page 173.
- Restart the server. Refer to Part 1 of the *CallPilot Installation and Configuration* binder, “Restarting the server.”

Taking remote control of the CallPilot server

Introduction

You can use pcAnywhere to operate the server as if you were directly connected to it.

ATTENTION

Do not schedule intensive remote tasks during peak traffic hours. This can adversely affect call processing capabilities of the CallPilot server.

Before you begin

- If the server is not on the same LAN as the remote personal computer, establish a dial-up connection over the PSTN. See “Establishing a connection using Dial-Up Networking” on page 168.
- Obtain the password for a remote access user account (for example, the NGenDist user account) and pcAnywhere caller account on the server (for example, the NGenDist caller account).

Restarting the server using pcAnywhere

If pcAnywhere is installed, establish a remote control session and restart the server using the Windows shutdown operation.

See also

For specific instructions on using the pcAnywhere client to take remote control of a host, refer to the Symantec pcAnywhere documentation.

Optimizing remote host response during a pcAnywhere session

Introduction

Operating a remote host over a pcAnywhere connection can be slow because of public network traffic.

To speed up the response after you have established the connection, you can

- reduce the number of colors displayed during the session
- disable the host desktop

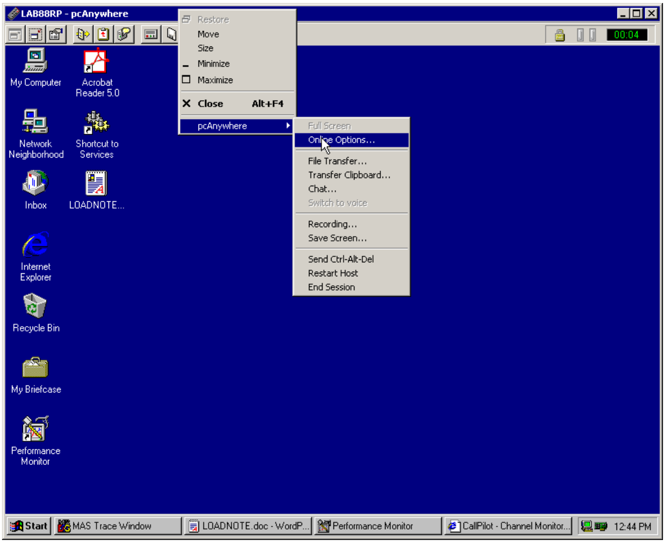
To optimize response of the remote host

1 Right-click the menu bar of the session window.

Result: A menu appears.

2 Click **pcAnywhere**.

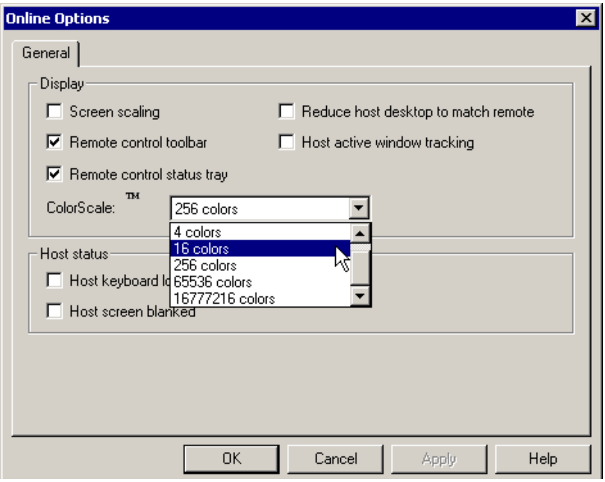
Result: The pcAnywhere options menu appears.



3 Click **Online Options**.

Result: The Online Options window appears.

4 To reduce the number of colors displayed during the session: in the **ColorScale** list, click **16 colors**.



Online Options

General

Display

□ Screen scaling
☑ Remote control toolbar
☑ Remote control status tray
□ Reduce host desktop to match remote
□ Host active window tracking

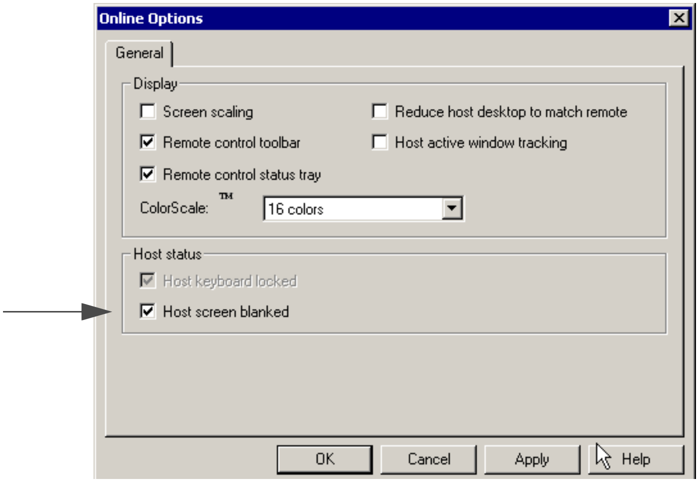
ColorScale:™ 256 colors

4 colors
16 colors
256 colors
65536 colors
16777216 colors

Host status

□ Host keyboard lo
□ Host screen blanked

5 To disable the host desktop: in the Host Status area, enable **Host Screen Blanked**.



Online Options

General

Display

□ Screen scaling
☑ Remote control toolbar
☑ Remote control status tray
□ Reduce host desktop to match remote
□ Host active window tracking

ColorScale:™ 16 colors

Host status

☑ Host keyboard locked
☑ Host screen blanked

6 Click OK.

Ending a dial-up connection

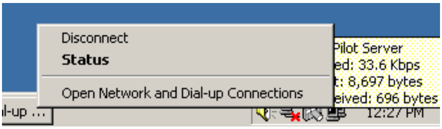
Introduction

When you end a dial-up connection to a CallPilot server, ensure that the server will be able to accept subsequent calls.

To end a dial-up connection

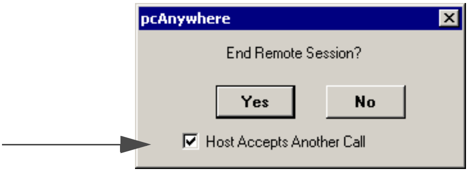
1 Right-click the icon on the toolbar.

Result: A menu appears.



2 Click **Disconnect**.

Result: A confirmation box appears.



3 Enable **Host Accepts Another Call** and then click **Yes**.

Part 2

Securing the CallPilot system

In this part

Chapter 6

CallPilot security recommendations

In this chapter

Recommendations and references

- Treat CallPilot servers as closed systems.

ATTENTION

If you install unauthorized software on any CallPilot server, you might

- incur security problems
- conflict with CallPilot services
- prevent the CallPilot server from functioning properly

- Ensure that each CallPilot server is physically secured.

  Refer to Part 2 of the *CallPilot Installation and Configuration* binder for your server model.
- Ensure that all CallPilot backup tapes are physically secured.
- Ensure that all Windows NT account passwords are changed from their default values to strong values known only by the customer. This includes the *gamroot* account used for the AR352 RAID card.

  Refer to Parts 3 and 5 of the *CallPilot Installation and Configuration* binder for your server model.
- Always run the CallPilot server with its console in a logged out state.
- When you configure a remote disk destination on your LAN, you map the remote drive onto the CallPilot server.

ATTENTION

Do not map a CallPilot server drive onto another server. This applies to all connections to the server regardless of location (across the hall via the LAN or across the country on the WAN).

- When you configure a remote disk destination on your LAN, you create NGenSys as a user on the remote file server.

ATTENTION

Do not add users or shares to a CallPilot server.

- Ensure that the CallPilot server is connected *inside* the customer's LAN firewall.

  Refer to Part 1 of the *CallPilot Installation and Configuration* binder.
- Install and configure one of the Nortel Network-approved third party anti-virus solutions according to Nortel recommendations.

ATTENTION

Do not install third party anti-virus software unless it has been approved by your IT department.

Refer to the *CallPilot General Release Bulletin*.

- When you initiate a dialup connection to use a third-party program such as pcAnywhere to perform remote administration on the CallPilot server, you need to enable the remote access modem on the server.

ATTENTION

Enable the remote access modem on the CallPilot server *only* when it is needed to enable a dialup connection for remote maintenance of the server.

See Chapter 5, "Configuring dial-up access to the CallPilot server" for more information.

Chapter 7

Physically securing your equipment and data

In this chapter

Overview

Introduction

This chapter describes some of the measures to take to make your work environment, equipment, and printed data more secure.

Securing the premises

Introduction

Physical security threats include

- events that can physically damage equipment
- ways in which equipment can be physically accessed to get to information.

When considering physical security, think not only of network media such as cabling and servers but also of physical resources and access controls.

Guidelines

Here are some guidelines for increasing the security of your workplace:

- Do not let visitors roam freely.
- If tours of the office are conducted, ensure that employees are aware of them. Sensitive data must not be left on computer screens or desktops.
- When people claim they are contractors or technicians, ask for identification. Verify that they are supposed to be there.
- Decide on a policy for after-hours access to your facilities, and educate employees. Do not leave it up to employees to decide who can come in and when.

See also

The “Site Inspection Checklist” in Part 1 of the *CallPilot Installation and Configuration* binder for your server model.

Securing equipment

Introduction

Set up a security policy to identify the measures that are put into place to secure equipment.

The equipment room

Try to keep all servers and other critical equipment in a room (or rooms) that can be locked. If an equipment room is used for several purposes, consider separate rooms. Here are more guidelines for securing equipment rooms:

- Give access to equipment rooms to authorized personnel only. Security badges and a badge reader that records the time and identity of each person entering the room are highly recommended.
- If the equipment room has ceiling tiles, ask your building's maintenance company to either secure them or extend the wall through the ceiling.
- Keep track of keys or badges that are used to gain entry. When employees leave your company, cancel the access privileges they had.
- Install hidden video cameras.
- Ensure the room has adequate ventilation and cooling. An overheated room can cause mechanical parts to break down. You can also purchase temperature sensors that page you when the temperature fluctuates a certain amount.
- Do not allow cleaning staff to enter the room. If there is a trash can in the room, set it outside when it gets full. Make sure the can contains no sensitive information.

Cabling and wiring

Cables and wiring present another potential security threat:

- Plan wiring runs, and make them difficult to access.
- Do not leave cabling exposed. Check your premises regularly for loose, exposed, or insecure cabling. Check for cable drops that are inactive, and disconnect them from your hubs until needed.
- Your building's wiring system can be tapped, and electronic emissions can be picked up. Any wiring leading from a computer to the building wiring must be shielded.

Remote personal computers

Remote personal computers can be vulnerable if not properly protected:

- Use power-on passwords that require a user to enter a password before the system will start. They prevent someone from using a DOS boot disk, inserted in a floppy drive, to bypass the regular boot process.
- Educate users about using passwords and screen savers properly.
- If you give older workstations away or trade in older equipment, be sure to wipe the hard drives with specialized tools. Hard drives that contain sensitive or classified information must be destroyed.

Disposing of printed information

Introduction

Hackers and criminals search through trash to obtain useful or sensitive information. Develop a policy for disposing of information and educate employees about it.

Guidelines

Keep important information from ending up in your trash by following these guidelines:

- Identify reports that contain sensitive information, access codes, or passwords. Make sure these reports are shredded.
- You must check file folders that are being thrown out for papers that might have been left in them.
- Shred any network diagrams (that can show where routers are, which ports are blocked, and so on) before throwing them out. While they are still in use, keep these diagrams locked up.

Chapter 8

Backing up and restoring CallPilot information

In this chapter

Overview

Introduction

Before you back up or restore CallPilot data, understand how an archive differs from a system backup. Then, familiarize yourself with the considerations and guidelines.

This overview discusses

- benefits of performing CallPilot server backups and archives
- backup schedules
- backup devices (destinations)
- backup speed

Benefits

Perform full system backups frequently and at regular intervals to prevent data loss so that you can

- save and restore a complete set of system and multimedia data files from your CallPilot server, in the event of disk drive failure or corrupted or lost configuration and messaging data
- protect against data loss due to theft or damage caused by natural disasters

ATTENTION

Nortel Networks recommends that you schedule periodic backups (even on servers equipped with RAID) because

- Backups protect against data loss due to software problems (for example, file system corruption, registry corruption, or failed upgrades), undetected disk errors, double faults, and human error.
- Backups and archives are useful for migration to a different CallPilot platform.

Use archives to

- Support recovery from inadvertent deletions of a user’s messages or mailbox, personal distribution lists (PDLs), greetings, personal verifications, customized prompts, and custom applications.
- Import custom applications from another system.
- Import mailboxes from another system.

Note: You can restore data from an archive without taking the CallPilot system out of service.

Backup schedules

Use the CallPilot Manager System Backup/Restore option to schedule periodic backups.

When to perform or schedule backups

Perform or schedule backups at the following times:

- before and after major system operations take place, such as an upgrade or the installation of performance enhancement packages (PEPs)
- after you make any major modifications, such as the addition of a large number of mailboxes, customized prompts, or custom applications.
- at regular intervals during normal operation, according to the criticality of your message data

ATTENTION

To avoid backup failure, do not schedule backups during the MMFS audit hour (3:00 a.m. to 4:00 a.m., server time) or during peak traffic hours.

Backup devices (destinations)

You can back up files either to the server tape or to disk space on a computer on the customer LAN. If the backup device that you want to specify is not listed, you must define it as a new backup destination.

When you define a backup, you must specify a destination backup device that is listed in the Backup Browser (Devices view).

ATTENTION

CallPilot does not support backups to

- local disks
- remote disks on computers running Windows 95

Predefined backup device

When the CallPilot server software is installed, only the system backup tape is predefined as a backup device. This device appears automatically in the Backup Browser (Devices view).

Backup speed

The speed with which backups are performed depends on

- system traffic
- whether the backup device is local

See “Total Backup Elapsed Time table” on page 205.

Guidelines for backing up and restoring CallPilot data

A well-planned backup/archive strategy minimizes the risk of losing data. Consider the following:

- Which data is critical to the organization and should be backed up?
- How often does data change?
- How can impact on the system be minimized?
- How can the safety of backups be ensured?

Which data is critical to the organization and should be backed up?

- Perform full system backups frequently and at regular intervals (even on servers equipped with RAID) to prevent data loss.
- Update user archives frequently and at regular intervals.
- Update Application Builder (custom application) archives periodically and whenever applications are added or updated.
- Update prompt archives whenever voice prompts are added or updated.

How often does data change?

- Use a weekly or monthly schedule to periodically back up data that changes infrequently.
- Use a daily schedule to back up data that changes constantly more often, especially if it is critical to the organization.
- When new applications are created, they are not automatically added to existing application archives. You must redefine the application archive in which the new application belongs

How can impact on the system be minimized?

- Because backups compete with services for system resources, schedule backups to run during off-peak hours, even though running a backup at peak hours has a minimal impact on response time. To determine the peak call processing periods, use Reporter to run a report.
- Consult the “Total Backup Elapsed Time table” on page 205.

How can the safety of backups be ensured?

- Do not attempt to use third-party backup utilities to back up CallPilot server information. They might interfere with CallPilot files and stop call processing.
- Do not perform administrative tasks while a backup is in progress. That work might be lost in the event that the backup is used to restore CallPilot server information.
- You must ensure that the backup was completed with no errors before you can assume that the backup is usable. Check the log files or the Alarm Monitor for errors. See “Checking the details of a backup or restore operation” on page 198.
- Store your backup media in an environment that meets the media manufacturer’s storage requirements.
- Determine both onsite and offsite locations for backup media.
- Ensure that only authorized personnel have full access to the sites.
- Ensure that those responsible for maintaining backups fully understand their roles.
- Be sure they know how to label backup media for easy retrieval.
- All backup tapes must be specially formatted for CallPilot server backup data. When you schedule a full system backup, select “Backup will overwrite any existing data on the tape.” The overwrite process formats the tape for CallPilot server backups.
- If you schedule your system backup and your secondary disk backups (TRP three-drive systems only) at different times, but intend to use the same tape, append the data. Do not overwrite the existing data.

Restoring from full system backups

Introduction

Your distributor is responsible for using your system backups to return the server to the state it was in when the backup was created.

You can restore information from an archive as you need to.

Restoring your CallPilot system from the base hardware

When you receive your server from the factory, some software, such as the operating system and the CallPilot server software, is already installed. The installation instructions in the Installation and Configuration Guide for your server begin where the factory installation stops.

Refer to Part 4: Installation and Configuration Guide, “Software Installation and Maintenance” for the information you need to reinstall a complete system from scratch.

ATTENTION

In the case of a complete system failure, contact your CallPilot distributor. Your CallPilot distributor and your system administrator can use a support tool to rebuild your system from the base hardware up.

Monitoring the status of a backup or restore operation

Introduction

When you have successfully started a backup or restore operation, CallPilot Manager shows the current status of the operation.

ATTENTION

If the backup or restore operation was scheduled for a specific date and time, select Status from the View list.

CallPilot Manager also displays the following information:

- number of records backed up
- number of records to be backed up
- and number of errors.

The icon indicates the current CallPilot server status.

Icon	State of the backup or restore operation
⌛	Operation is running OR Cancel request by the administrator is pending
✗	Operation was canceled because of fatal errors OR Operation was canceled by the administrator
✓	Operation was completed successfully
✓	Operation was partially completed OR Operation was completed with errors

Note: If there is no icon, no backup or restore operation is running.

What to do if there are errors

Whenever there are errors, view the error log that is generated for the operation.

Checking the details of a backup or restore operation

Introduction

When you need to view the details of a backup or restore operation, you can use either the CallPilot Manager histories or the logs that are automatically created on the CallPilot server during a backup or restore operation.

Histories

You can use CallPilot Manager to display histories for

- all system backups
- all archive backups and restores
- application archive backups and restores
- prompt archive backup and restores
- user archive backups and restores

Backup and restore histories provide the following information:

- Name of the operation
- Completion Status
- Date
- Elapsed Time (HH:MM:SS)
- Type
- Total Size (KB)
- Device (destination)
- Primary Error
- Extended Error

If the history does not provide adequate detail, check the log.

ATTENTION Histories are deleted automatically after 90 days.

Logs

The logs are more detailed than the CallPilot Manager histories.

- The backup log files are located in D:\nortel\data\backup\BackupLogs
- The restore log files are located in D:\nortel\data\backup\RestoreLogs

Configuring a new backup destination on the network

Introduction

The network must be configured to allow backups to be performed to a remote disk drive on a computer running Windows 98/NT/2000.

ATTENTION

CallPilot does not support backups to

- local disks
- remote disks on computers running Windows 95

What you need before you can configure a remote disk destination

- access to the remote file server
- the NGenSys password configured on the CallPilot server

Configuring the network to allow backups to a remote disk

There are two steps to configuring the network to allow backups to a remote disk.

1. On the remote file server, create a writable share that is accessible only to the CallPilot server.
2. On the CallPilot server, map a drive to the remote file server.

Looking up procedures in CallPilot Manager online Help

Find procedures for scheduling and performing backups by looking up **server backups** in the Index.

ATTENTION

The procedure steps in the online Help are high-level and include examples of how windows are completed. For specific instructions that apply to the Windows operating system you are using, refer to your Windows online Help.

Scheduling backups to tape or disk

Introduction

After the CallPilot server is installed and operational, schedule periodic server backups. You can also define one-time server backups. Once these backups are defined, They run automatically at the scheduled time.

ATTENTION

To avoid backup failure, do not schedule backups during the MMFS audit hour (3:00 a.m. to 4:00 a.m., server time) or during peak traffic hours.

Regularly verify that backups are successful. See “Checking the details of a backup or restore operation” on page 198.

IPE system backups

All IPE systems are shipped with one drive.

Table of IPE system backup options

The following table describes your IPE system backup type options:

Backup type	Description
Full System Backup	Backs up the entire system.
User Archive	Backs up all mailbox messages, personal information, greetings, personal verifications, and personal distribution lists (PDLs).
Prompt Archive	Backs up all custom prompts.
AppBuilder Archive	Backs up all custom applications.

Tower and rackmount system backups

Tower and rackmount systems are shipped in either of the two following configurations:

- a server with only one drive
- a server with three drives

If your TRP system has three drives, you can back up the entire system, or you can back up a specific drive. This option is useful if a drive will be replaced.

Table of tower and rackmount system backup options (one drive)

The following table outlines your tower and rackmount system backup type options if your TRP system has only one drive:

Backup type	Description
Full System Backup	Backs up the entire system.
User Archive	Backs up all mailbox messages, personal information, greetings, personal verifications, and personal distribution lists (PDLs).
Prompt Archive	Backs up all custom prompts.
AppBuilder Archive	Backs up all custom applications.

Table of tower and rackmount system backup options (three drives)

The following table outlines your tower and rackmount system backup type options if your system has three drives:

Backup type	Description
Full System Backup	Backs up the entire system.
Backup of D drive	Backs up the contents of D drive.
Backup of E drive	Backs up the contents of E drive.
Backup of F drive	Backs up the contents of F drive.
User Archive	Backs up all mailbox messages, personal information, greetings, personal verifications, and personal distribution lists (PDLs).
Prompt Archive	Backs up all custom prompts.
AppBuilder Archive	Backs up all custom applications.

Configuring backups to the system backup tape

When you schedule backups to the system backup tape, you must specify whether to overwrite the contents of the tape or append the new data to the contents of the tape.

When to overwrite data and format the tape

All backup tapes must be specially formatted for CallPilot server backup data. When you schedule a full system backup, select “Backup will overwrite any existing data on the tape.”

The overwrite process formats the tape for CallPilot server backups.

ATTENTION

To ensure the integrity of your full system backups, use a new tape for each backup.

When *not* to overwrite data

If you schedule your system backup and your secondary TRP disk backups at different times, but intend to use the same tape, select “Backup will be appended after existing data on the tape.” This will ensure that the new backup data is appended to the existing contents of the tape.

Determining a time slot for a full system backup

To minimize impact on system performance, schedule backups and large archives during periods of light traffic.

Use the table in the following section to help determine, for each platform, the best times to schedule full system backups.

Total Backup Elapsed Time table

The following table lists the estimated times required to back up all system and archived data for the largest possible system on each supported platform.

Platform	Tape drive	Tape cartridge	Maximum storage (hours)	Estimated time for full backup (hh:mm)
200i	SLR5	SLR5	200	1:58
201i	SLR5	SLR5	350	2:55
702t	SLR32	SLR32	1000	1:56
702t	SLR50	SLR32	1000	1:56
702t	SLR50	SLR50	1000	1:28
1001rp	SLR32	SLR32	1000	1:56
1001rp	SLR50	SLR32	1000	1:56

Platform	Tape drive	Tape cartridge	Maximum storage (hours)	Estimated time for full backup (hh:mm)
1001rp	SLR50	SLR50	1000	1:28
1002rp	SLR50	SLR50	2400	1:42

Looking up procedures in CallPilot Manager online Help

- Find procedures for scheduling and performing backups by looking up **server backups** in the Index.
- Find procedures for scheduling and performing archives by looking up **archives** in the Index.

Performing an immediate backup to tape or disk

Introduction

Instead of scheduling a backup to run in the future, you can run an existing backup to save vital and current data immediately.

You must have an existing backup or archive definition in which to save the data.

When to perform an immediate backup

- Perform immediate server backups
  - before and after hardware repairs
  - before and after system upgrades
- Perform immediate secondary TRP drive backups before and after disk drive replacements.
- Perform immediate backups to Application Builder (custom application) archives whenever applications are added or updated.
- Perform immediate backups to prompt archives whenever voice prompts are added or updated.
- Perform immediate backups to user archives whenever large numbers of mailboxes have been added, deleted, or updated.

Precautions

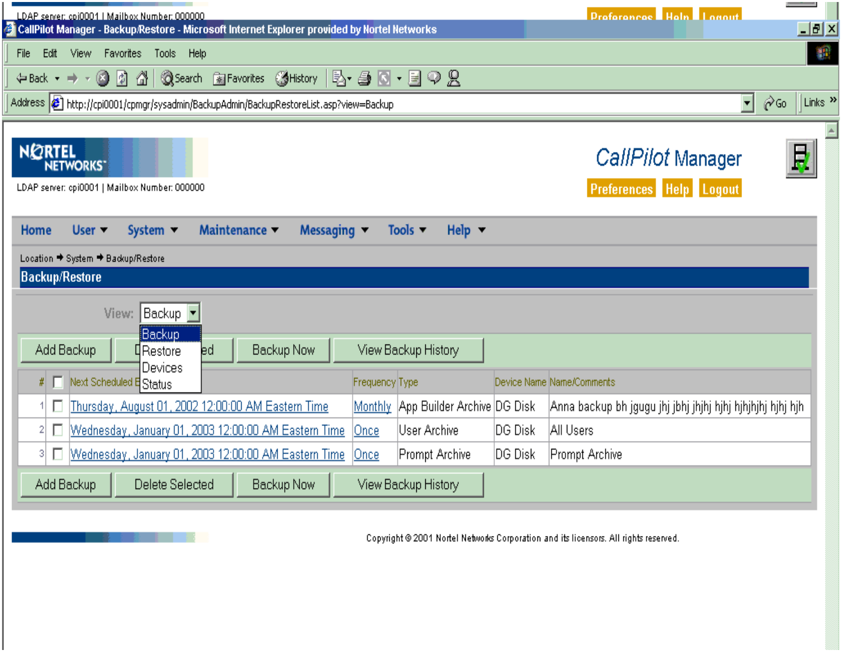
- To avoid backup failure, do not schedule backups during the MMFS audit hour (3:00 a.m. to 4:00 a.m., server time) or during peak traffic hours.
- Regularly verify that backups are successful. See “Checking the details of a backup or restore operation” on page 198.

Before you can perform an immediate full system backup

Ensure there is a backup listed in the schedule that is defined the way you need it for the immediate system backup.

When you add a backup to the schedule, use the Comments field to indicate whether the definition is suitable for an immediate backup.

Getting there System → Backup/Restore


CallPilot Manager - Backup/Restore - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/sysadmin/BackupAdmin/BackupRestoreList.asp?view=Backup
Go Links
NORTEL NETWORKS
LDAP server: cpi0001 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location ➔ System ➔ Backup/Restore
Backup/Restore
View: Backup
Backup
Restore
Devices
Status
Add Backup
Backup Now
View Backup History
Delete Selected

#	□	Next Scheduled E	Frequency	Type	Device Name	Name/Comments
1	□	Thursday, August 01, 2002 12:00:00 AM Eastern Time	Monthly	App Builder Archive	DG Disk	Anna backup bh jgugu jhj jbhj jhjhj hjhj hjhjhjhj hjhj hjh
2	□	Wednesday, January 01, 2003 12:00:00 AM Eastern Time	Once	User Archive	DG Disk	All Users
3	□	Wednesday, January 01, 2003 12:00:00 AM Eastern Time	Once	Prompt Archive	DG Disk	Prompt Archive

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

Looking up procedures in CallPilot Manager online Help

Find procedures for scheduling and performing backups by looking up **server backups** in the Index.

Find procedures for scheduling and performing archives by looking up **archives** in the Index.

Changing the backup destination

Introduction

You can back up files either to the system backup tape or to a remote disk.

When you add a backup operation to the schedule, you must specify a destination device that is listed in the Device Name list in the Backup Browser (Devices view).

The system backup tape is automatically listed in the Backup Browser (Devices view) when the CallPilot server software is installed. If you want to back up the server to a disk device, that device must be defined as a new backup destination.

Backups to a remote disk drive

The network must be configured to allow backups to be performed to a remote disk drive on a Windows 98/NT/2000 remote file server.

ATTENTION

CallPilot does not support backups to

- local disks
- remote disks on computers running Windows 95

Information you need to add a disk backup destination

- device name
- path to the destination device:
  - remote computer name
  - share name

Path names

When you add a backup device that represents disk space, you must enter the path.

For remote disk directories, enter the universal naming convention path.

Example

\\SERVER1\BACKUPDATA, where

- SERVER1 is the computer name
- BACKUPDATA is the share name

ATTENTION

CallPilot does not support backups to

- local disks
- remote disks on computers running Windows 95

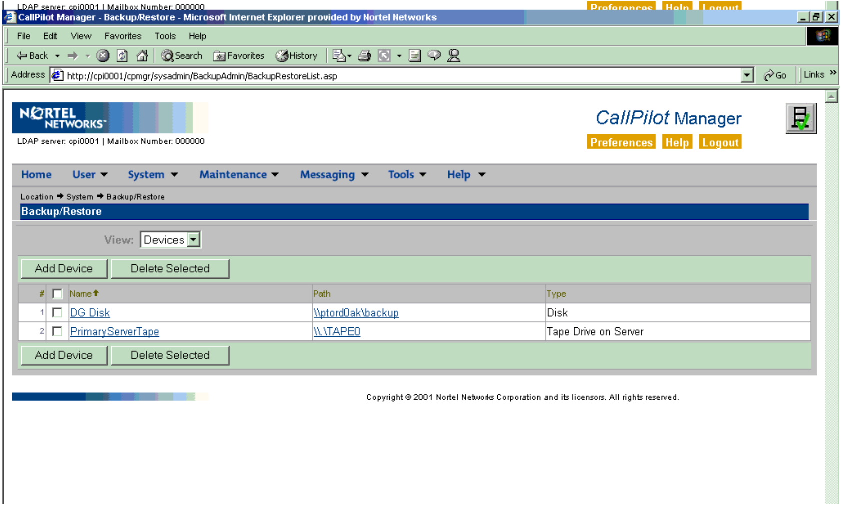
Share names

The share name is not the same as the name of the shared folder.

To find the share name:

1. Connect to the remote computer and locate the shared folder.
2. Right-click the folder name and click Properties.
3. Click the Sharing tab and view the Share Name.

Getting there System → Backup/Restore → Devices


CallPilot Manager - Backup/Restore - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/sysadmin/BackupAdmin/BackupRestoreList.asp
Go Links
NORTEL NETWORKS
LDAP server: cpi0001 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location → System → Backup/Restore
Backup/Restore
Add Device Delete Selected
Copyright © 2001 Nortel Networks Corporation and its licensors. All rights reserved.

View: Devices

#	□	Name	Path	Type
1	□	DG Disk	\\ptord0ak\backup	Disk
2	□	PrimaryServerTape	\\.\TAPE0	Tape Drive on Server

Looking up procedures in CallPilot Manager online Help

Find procedures for changing the Device Name list by looking up **server backups** in the Index.

Restoring from full system backups

Introduction

Your distributor is responsible for using your backups to return the server to the state it was in when the backup was created.

Restoring your CallPilot system from the base hardware

When you receive your server from the factory, some software, such as the operating system and the CallPilot server software, is already installed. The installation instructions in the *CallPilot Installation and Configuration* binder for your server model begin where the factory installation stops.

ATTENTION

In the case of a complete system failure, contact your CallPilot distributor.

Your *CallPilot Installation and Configuration* binder also contains the information you must reinstall a complete system from scratch. Your CallPilot distributor and your system administrator can use the information in the *CallPilot Installation and Configuration* binder to rebuild your system.

Using CallPilot archives

Introduction

Archives are copies of multimedia files from CallPilot. Archives specifically back up Application Builder applications, personal user data (such as greeting, messages, and personal distribution lists), and customized voice prompts.

Use archives to

- Support recovery from inadvertent deletions of a user’s messages or mailbox, personal distribution lists (PDLs), greetings, personal verifications, customized prompts, and custom applications.
- Port custom applications from another system.
- Port mailboxes and administrators from another system.

See also

“Backup and restore capabilities” on page 68.

Types of archives

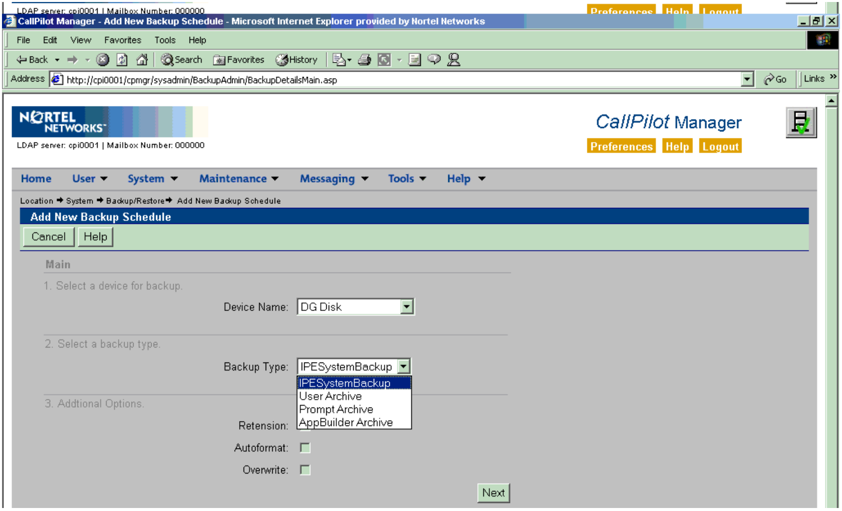
CallPilot supports the following archive types:

- *User archives* store all CallPilot configuration information about mailboxes, mailbox owners, and administrators. You can select the information to include in a single archive by defining search criteria for the archive.
- *Prompt archives* store all custom prompts recorded in a single language.
- *AppBuilder archives* store custom applications created using Application Builder.

Limitations

- Archives do not save switch-related setup, operational measurement data, event logs, alarms, system security settings, the networking setup, or queues of undelivered and time-delayed messages.
- If you restore one or more messages from a user archive, they are added to the messages that are currently in the destination mailbox. The mailbox owner may complain that deleted messages re-appear in the mailbox.
- You cannot selectively restore customized prompts from a prompt archive.

Getting there: System → Backup/Restore → Add Backup



CallPilot Manager - Add New Backup Schedule - Microsoft Internet Explorer provided by Nortel Networks

Address http://cpi0001/cpmgr/sysadmin/BackupAdmin/BackupDetailsMain.asp

LDAP server: cpi0001 | Mailbox Number: 000000

Location ➔ System ➔ Backup/Restore➔ Add New Backup Schedule

Add New Backup Schedule

Main

1. Select a device for backup.

Device Name: DG Disk

2. Select a backup type.

Backup Type: IPESystemBackup

3. Addtional Options.

Retension:

Autoformat: □

Overwrite: □

Looking up procedures in CallPilot Manager online Help

Find procedures for backing up to, restoring from, and viewing archives by looking up **archives** in the Index.

Using mailbox (user) archives

Introduction

Most customers define a single user archive for all mailbox information and schedule the archive to run daily, during a period of light system traffic. See “Archive Capacity table” on page 218.

You can use archived mailbox information to import mailboxes from another CallPilot server.

You can define each user archive to back up only the mailboxes and administrators that you select.

Dynamic archive capability

When you add or delete mailboxes or administrators, you do not have to manually add or delete them to or from a user archive that has been defined to store information that includes the new information. This is because the user archive backup process employs CallPilot Manager search functions to automatically update the archive as you back up information. See “Guidelines for defining a set of user archives” on page 217.

Example

The Information Technology (IT) department employs two co-operative education students per quarter. When a new quarter begins, the currently employed students in the department return to university classes and two different students take their place.

User archives are defined by department, so that mailbox information for all IT department employees are stored in the 9B2T (IT) archive. The search criterion that determines the contents of the archive is “Department EQUALS 9B2T (IT).” This means that each time information is backed up to the 9B2T archive, the search is regenerated. Information pertaining to the former co-op students is automatically left out and information pertaining to the new co-op students is automatically added.

Upgrading from CallPilot 1.07 to CallPilot 2.0

If you are upgrading from CallPilot 1.07 to CallPilot 2.0, you can use your CallPilot 1.07 user archives to migrate mailbox information to the new platform.

ATTENTION

When you are restoring a CallPilot 1.07 user archive to a CallPilot 2.0 server, be aware that mailbox owners with remote notification capability are automatically given remote text notification capability.

Impact on system performance

Note that performing an archive is a computer-intensive task and should only be performed during low traffic periods. Most customers experience no noticeable impact on system performance. If you do notice an impact on system performance, see the CallPilot Manager online Help Troubleshooting topic “Archiving mailbox information slows down the system.”

Limitations

- Archives do not save switch-related setup, operational measurement data, event logs, alarms, system security settings, the networking setup, or queues of undelivered and time-delayed messages.
- If you restore one or more messages from a user archive, they are added to the messages that are currently in the destination mailbox. The mailbox owner may complain that deleted messages re-appear in the mailbox.

Defining sets of user archives

If your system has more mailboxes than the number recommended to archive on the device you have configured (disk or tape), define a set of user archives where each archive contains no more than the recommended number.

Example: If your 1002rp system has 12000 mailboxes, you must define at least three archives and ensure that none has more than 5000 mailboxes backed up. Allow three Gbytes for each of the three archive segments.

You can define each user archive to back up only the mailboxes and administrators that you select.

Guidelines for defining a set of user archives

You can define a user archive around any of the user search criteria. For example, you can

- define a separate archive for administrators
- define a different archive for each department or location
- archive mailboxes in numeric segments (for example, mailboxes 7*, 8*, and so forth)
- archive mailbox owners by last name in alphabetic segments (for example, a*, b*, . . . , z*)

Determining a time slot for a backup to a user archive

These recommendations are based on the assumption that there is a period of eight contiguous hours of light system traffic.

To arrive at the calculations shown in the Archive Capacity table, each test mailbox consisted of

- five voice messages, each 40 seconds in length
- Personal Greetings
- Personal Verification
- no PDL

Archive Capacity table

Platform	Maximum number of mailboxes	Maximum number of mailboxes to archive in a single segment		Gbytes required for each segment
		On disk	On tape	
200i	8000	2500	2500	2.5
201i	10000	3000	3000	2.5
702t	20000	4000	4000	3
1001rp	20000	4000	4000	3
1002rp	50000	5000	5000	4

Looking up procedures in CallPilot Manager online Help

Find procedures for backing up to and restoring to user archives by looking up **user archives** in the Index.

Using prompt archives

Introduction

Define at least one prompt archive for each language installed on your CallPilot server. Back up prompt information to these archives each time prompts are updated.

ATTENTION

When new applications are created, they are not automatically added to existing application archives. You must use the procedure in this topic to redefine the application archive in which the new application belongs.

Limitations

Archives do not save switch-related setup, operational measurement data, event logs, alarms, system security settings, the networking setup, or queues of undelivered and time-delayed messages.

ATTENTION

You cannot selectively restore customized prompts from a prompt archive.

Looking up procedures in CallPilot Manager online Help

Find procedures for backing up to and restoring from prompt archives by looking up **prompt archives** in the Index.

Using application archives

Introduction

Define at least one application archive and back up to application archives weekly.

ATTENTION

When new applications are created, they are not automatically added to existing application archives. You must use the procedure in this topic to redefine the application archive in which the new application belongs.

Recommendation

Consider defining separate archives for

- voice menus (by language)
- applications for different functions (such as those using the Application Builder Thru-Dial block)

Limitations

Archives do not save switch-related setup, operational measurement data, event logs, alarms, system security settings, the networking setup, or queues of undelivered and time-delayed messages.

Looking up procedures in CallPilot Manager online Help

Find procedures for backing up from and restoring to application archives by looking up **AppBuilder archives** in the Index.

Restoring from archives

Introduction

You can restore data from an archive without taking the CallPilot system out of service.

Limitations

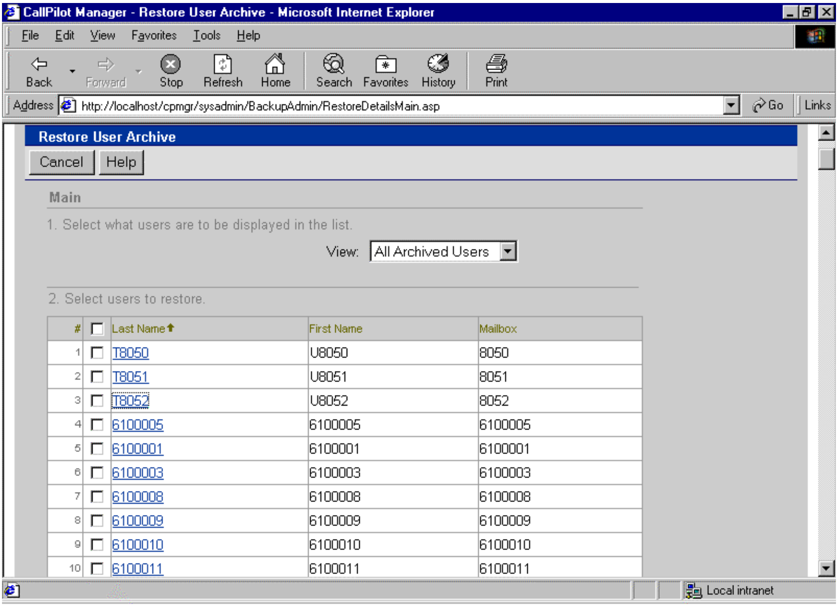
- Archives do not save switch-related setup, operational measurement data, event logs, alarms, system security settings, the networking setup, or queues of undelivered and time-delayed messages.
- If you restore one or more messages from a user archive, they are added to the messages currently in the destination mailbox. The mailbox owner may complain that deleted messages re-appear in the mailbox.
- Custom commands and personal verifications cannot be restored from a user archive.
- You cannot selectively restore customized prompts from a prompt archive.

Choosing from a list of archives

When you restore data from an archive, you choose from a list of the type of archive you have selected.

The following illustration shows a list of user archives.

Getting there System → Backup/Restore → Restore → Backup Device → Retrieve Directory


CallPilot Manager - Restore User Archive - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Print
Address
Go
Links
Cancel
Help
Local intranet

Address: http://localhost/cpmgr/sysadmin/BackupAdmin/RestoreDetailsMain.asp

Restore User Archive

Main

1. Select what users are to be displayed in the list.

View: All Archived Users

2. Select users to restore.

#	□	Last Name	First Name	Mailbox
1	□	T8050	U8050	8050
2	□	T8051	U8051	8051
3	□	T8052	U8052	8052
4	□	6100005	6100005	6100005
5	□	6100001	6100001	6100001
6	□	6100003	6100003	6100003
7	□	6100008	6100008	6100008
8	□	6100009	6100009	6100009
9	□	6100010	6100010	6100010
10	□	6100011	6100011	6100011

Looking up procedures in CallPilot Manager online Help

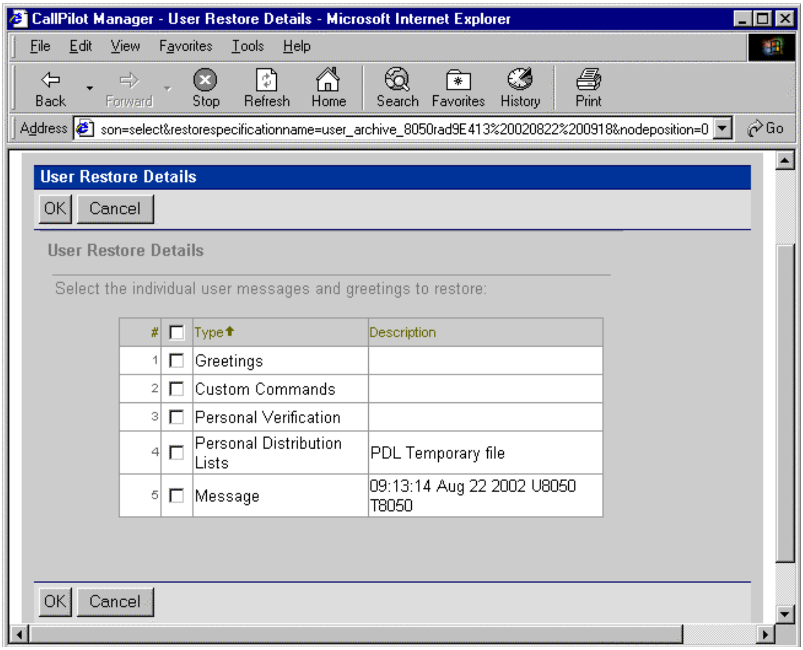
Find procedures for restoring from archives by looking up **archives** in the Index.

Selecting user information to restore

Once you have selected an archive, you can select specific information to restore.

The following illustration shows a detail from a user archive.

Getting there System → Backup/Restore → Restore → Backup Device → Retrieve Directory → User Restore Details


CallPilot Manager - User Restore Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Print
Address son=select&restorespecificationname=user_archive_8050rad9E413%20020822%200918&nodeposition=0
Go
OK Cancel

User Restore Details

User Restore Details

Select the individual user messages and greetings to restore:

#	□	Type	Description
1	□	Greetings	
2	□	Custom Commands	
3	□	Personal Verification	
4	□	Personal Distribution Lists	PDL Temporary file
5	□	Message	09:13:14 Aug 22 2002 U8050 T8050

Chapter 9

Monitoring suspicious activities

In this chapter

What to monitor and when

Introduction

If you have noticed suspicious activity on your system, use CallPilot Security Administration features to monitor CallPilot for certain events that you suspect are caused by hackers who have gained access to your system. When the event you are monitoring occurs, an alarm is generated. This means you are notified of suspicious activity in real time so you can investigate immediately.

When to enable monitoring

Generally, you enable activity monitoring only when you suspect hacker activity on your system.

You might be alerted to suspicious activities by

- mailbox owners complain of suspicious behavior, such as changed greetings or obscene messages
- an alert is triggered by Reporter
- a report generated in Reporter indicates unusual traffic or usage patterns

What you can monitor

You can monitor

- internal and external telephone numbers (CLIDs) from which you suspect hackers are calling
- mailboxes to which you suspect hackers have gained access
- custom applications that hackers may be using for unauthorized thru-dial activities
- SMTP/VPIM IP addresses, user IDs, and FQDNs

Notification of suspicious activity

You can find out about the alarms generated by

- viewing the Alarms Monitor regularly to learn of new alarms
- setting up an alarm mailbox so that whenever an alarm is generated, the system sends a voice message to the mailbox to alert you
- enabling remote notification for the alarm mailbox so you are notified of new alarm messages immediately at a specified number, such as a pager or cell phone

Monitoring mailbox logon and thru-dialing activities

Introduction

If you suspect abuse of mailbox privileges, you can monitor mailbox logon and thru-dialing activities.

After you have determined the cause of suspicious activity and have resolved the problem, remove the corresponding mailboxes from the monitoring list.

Note: An event code is generated, each time someone logs on to a mailbox or the thru-dial process transfers a call from it.

Alarms that can be generated

The following alarms are generated whenever a logon or thru-dial attempt originates from a monitored mailbox:

Event number	Description
55703	Unknown system error occurred while attempting to transfer a call for an Application Builder application OR Unknown system error occurred in the Call Transfer block of an Application Builder application.
55717	A Thru-Dial block uses name or both name and number dialing, but no name prefix is defined for the name dialing service.
55750	Successful login to a mailbox from a Directory Number (DN) monitored by Hacker Monitor.

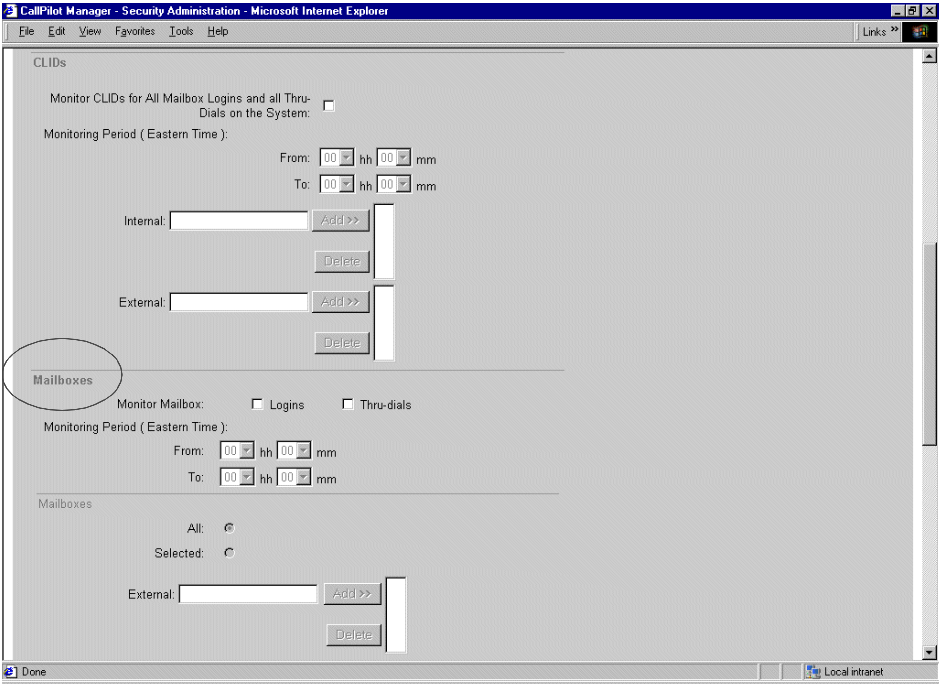
Event number	Description
55751	Failed login attempt to a mailbox from a Directory Number (DN) monitored by Hacker Monitor.
55752	A Thru-dial attempt was successful from a mailbox that is monitored by Hacker Monitor.
55753	A Thru-dial attempt was unsuccessful from a mailbox that is monitored by Hacker Monitor.
55756	A login attempt to a mailbox failed while Hacker Monitor was actively monitoring all mailboxes. The mailbox number is unknown.
55757	A login attempt to a mailbox failed while Hacker Monitor was actively monitoring all mailboxes. The mailbox number and Calling Line ID are unknown.
55758	Successful login to a mailbox that is being monitored by the Hacker Monitor.
55759	Successful login to a mailbox that is being monitored by the Hacker Monitor.
55760	Successful Thru-Dial from a mailbox that is being monitored by the Hacker Monitor.
55761	Successful Thru-Dial from a mailbox that is being monitored by the Hacker Monitor. The calling line ID is unknown.
55762	A Thru-Dial was attempted but not performed from a mailbox that is being monitored by the Hacker Monitor.
55763	A Thru-Dial was attempted but not performed from a mailbox that is being monitored by the Hacker Monitor.

For more info, see Event Code help

Monitoring options

You can specify individual mailboxes to track suspicious thru-dialing activities, logon attempts, or both. You can also specify a monitoring period.

Getting there: Messaging → Security Administration → Mailboxes settings


CallPilot Manager - Security Administration - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Links »
Add >>
Delete
Done
Local intranet

CLIDs

Monitor CLIDs for All Mailbox Logins and all Thru-Dials on the System: □

Monitoring Period (Eastern Time):

From: 00 hh 00 mm

To: 00 hh 00 mm

Internal:

External:

Mailboxes

Monitor Mailbox: □ Logins □ Thru-dials

Monitoring Period (Eastern Time):

From: 00 hh 00 mm

To: 00 hh 00 mm

Mailboxes

All: ●

Selected: ○

External:

Note: To display links to all Security Administration procedures, scroll to the bottom of the page and click the grey Help button.

Looking up information in CallPilot Manager online Help

Find procedures for adding and removing mailboxes from the list of mailboxes to be monitored by looking up **monitoring** in the Index.

To view the details for a specific event or return code

1 Click the Event in the Event Browser to open the Event Code Help.

2 If the help does not automatically display the desired information:

a. Click the Index tab in the left pane of this help file.

b. Type the event or return code as the keyword to find.

c. Press Enter. The code is located in the index list.

d. Click the code in the index list. The right pane refreshes to display the details for the specified event or return code.

Note: For more information, refer to the CallPilot Manager online Help topic “Event and return code help overview.”

Monitoring internal and external activity by calling line ID

Introduction

When a call comes in to the system, CallPilot keeps track of the calling line ID (CLID), if available. The CLID identifies a caller to the system. If you have identified certain CLIDs as suspicious (possibly the number from which a hacker is calling in to your system), you can use CallPilot Security Administration to monitor them.

How to identify suspicious CLIDs

You might become suspicious of certain CLIDs under the following conditions:

- You receive an Excessive After-Hours Logons alert. This alert reports the mailbox number and caller DN (the CLID).
- You run the Mailbox Call Session Summary report on mailboxes you suspect are targets of hackers and notice calls repeatedly originating from certain caller DNs.

Notification of access by monitored CLIDs

When thru-dial attempts are monitored, an alarm is generated whenever a monitored CLID gains access to the system and places an outgoing call. It does not matter how the call was transferred—whether it was from a mailbox or a custom application, for example.

All thru-dial activity that originates from the monitored CLID generates an alarm.

Alarms that can be generated

The following alarms are generated whenever a logon or thru-dial attempt originates from a monitored CLID:

Event number	Description
55750	Successful login to a mailbox from a Directory Number (DN) monitored by Hacker Monitor.
55751	Failed login attempt to a mailbox from a Directory Number (DN) monitored by Hacker Monitor.
55752	A Thru-dial attempt was successful from a mailbox that is monitored by Hacker Monitor.
55753	A Thru-dial attempt was unsuccessful from a mailbox that is monitored by Hacker Monitor.
55754	A Thru-dial attempt was successful from inside an Application Builder application.
55755	A Thru-dial attempt was unsuccessful from inside an Application Builder application.

For more info, see Event Code help

How to respond to alarms

If a specific mailbox is being targeted, determine if the mailbox is in use.

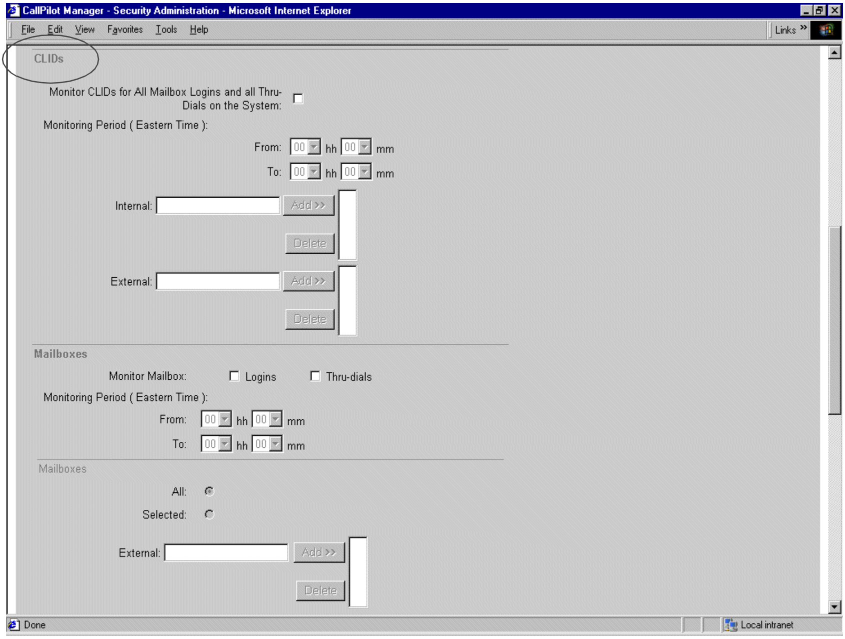
- If it is being used, inform the user and ask him or her to change the mailbox password immediately.
- If the mailbox is unused, delete it immediately.

Monitoring options

You can monitor

- all CLIDs for suspicious behavior, or you can specify certain CLIDs to be monitored
- logon or thru-dial attempts, or both
- for the entire day, or for a specified time period

Getting there: Messaging → Security Administration → CLIDs settings


CallPilot Manager - Security Administration - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Links
Add >>
Delete
Done
Local intranet

CLIDs

Monitor CLIDs for All Mailbox Logins and all Thru-Dials on the System: □

Monitoring Period (Eastern Time):

From: 00 hh 00 mm

To: 00 hh 00 mm

Internal:

External:

Mailboxes

Monitor Mailbox: □ Logins □ Thru-dials

Monitoring Period (Eastern Time):

From: 00 hh 00 mm

To: 00 hh 00 mm

Mailboxes

All: ●

Selected: ○

External:

Note: To display links to all Security Administration procedures, scroll to the bottom of the page and click the Help button.

Looking up procedures in CallPilot Manager online Help

Find procedures for monitoring all CLIDs and for selecting specific CLIDs to be monitored by looking up **monitoring** in the Index.

To view the details for a specific event or return code

1 Click the Event in the Event Browser to open the Event Code Help.

2 If the help does not automatically display the desired information:

a. Click the Index tab in the left pane of this help file.

b. Type the event or return code as the keyword to find.

c. Press Enter. The code is located in the index list.

d. Click the code in the index list. The right pane refreshes to display the details for the specified event or return code.

Note: For more information, refer to the CallPilot Manager online Help topic “Event and return code help overview.”

Monitoring suspicious SMTP activity

Introduction

You can use one of the following to monitor suspicious SMTP and VPIM Networking activity:

- the event log (automatic monitoring)

  If you choose to use the event log as your monitoring method, no action is required from you to initiate SMTP/VPIM monitoring.
- the Security Administration page in CallPilot Manager (manual monitoring)

Automatic monitoring

Automatic monitoring alerts you to suspicious SMTP activity, blocks access to the system, and provides sufficient information for further investigation. No configuration is required for automatic SMTP/VPIM monitoring.

You can use information collected by monitoring suspicious SMTP and VPIM Networking activity to

- Investigate the source of the suspicious activity.
- Enable manual hacker monitoring for the user ID, FQDN, or IP address.

How it works

When repeated unsuccessful authentication attempts are detected by CallPilot (for example, an incorrect password is presented), the following occurs:

IF the sender is a	THEN
local user	After the specified number of unsuccessful attempts, that user’s mailbox is disabled and an event is logged. Refer to the online Help topic “Configuring the authentication options on the local server.” **Note:** If the mailbox is disabled, the user cannot log in from either a phoneset or by using a desktop or web messaging client. Messages are no longer accepted via SMTP from that user, regardless of whether the user is authenticated or not.
remote server	After the specified number of unsuccessful attempts, message reception from the remote server is disabled and an event is logged. Refer to the online Help topic “Configuring the authentication options on the local server.” **Note:** If the remote server is disabled, messages from the remote server are no longer accepted.

Note: If the sender is presenting itself as a local mailbox or a remote server that does not actually exist, the system treatment is the same as when the mailbox or remote server does exist. This prevents the hacker from learning that the mailbox or server are not defined on the local system.

When the mailbox or server becomes disabled, an event is logged. The event includes the following information:

- the User ID (local mailbox number or remote server FQDN) used in the authentication attempt
- the FQDN and IP address from which the last authentication failure occurred

Monitoring activities manually

You can manually monitor activity based on the following:

- FQDN of the remote messaging server or desktop or web messaging client attempting to connect
- IP address of the remote messaging server or desktop or web messaging client attempting to connect
- authenticating user ID

You can define up to 100 activities to monitor. Monitoring provides you with a detailed list of activities received from the IP address, user ID, or FQDN. Activities that appear in the list include:

- all connections with successful authentication attempts
- all connections with unsuccessful authentication attempts
- all unauthenticated connections (that is, where authentication was not attempted)

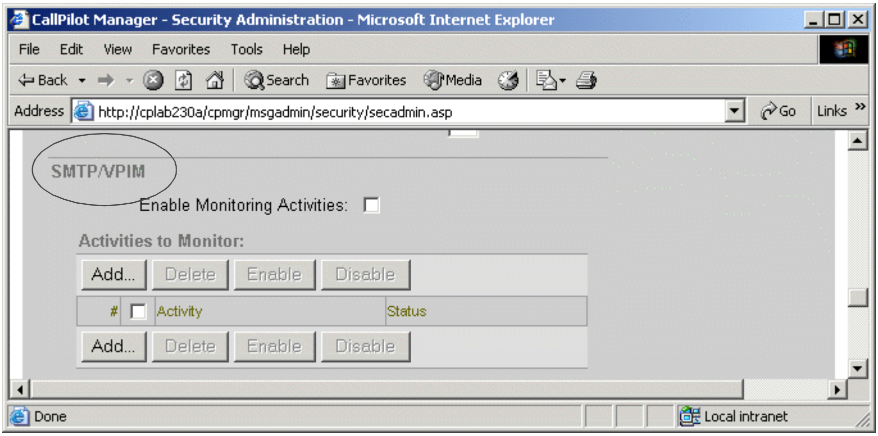
In addition to the activities list, an alarm message is deposited in the alarm mailbox, if the alarm mailbox is configured and these events have not been throttled.

When you have accumulated enough data about the hacker attack, you can disable monitoring of the offending source to avoid excessive logging. You can disable monitoring by using one of the following methods:

- Click Delete to remove the monitoring activity from the list.
- Click Disable to disable the monitoring activity.

  This retains the activity in the list so that you can enable it again, if required.

Getting there: Messaging → Security Administration → SMTP/VPIM settings


CallPilot Manager - Security Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://cplab230a/cpmgr/msgadmin/security/secadmin.asp
Go Links
SMTP/VPIM
Enable Monitoring Activities: □
Activities to Monitor:
Add... Delete Enable Disable
# □ Activity Status
Add... Delete Enable Disable
Done
Local intranet

To display links to all Security Administration procedures, scroll to the bottom of the page and click the Help button.

Looking up procedures in CallPilot Manager online Help

Find procedures for monitoring SMTP activity by looking up **monitoring** in the Index.

Find procedures for configuring authentication options for the CallPilot server, by looking up **SMTP authentication** in the Index.

Monitoring custom application SDNs

Introduction

You can monitor specified custom applications to track suspicious thru-dialing activities.

Note: An event code is generated each time there is thru-dialing activity from a custom application SDN.

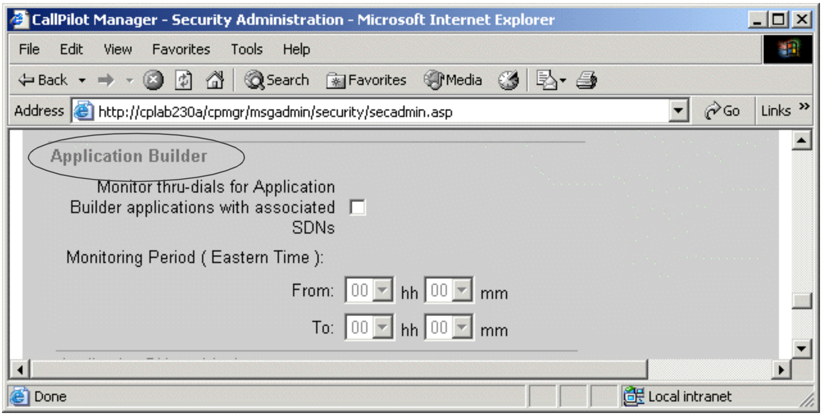
After you have determined the cause of suspicious activity and have resolved the problem, remove the corresponding application's SDN from the monitoring list.

Monitoring options

You can monitor

- all applications for suspicious behavior, or you can specify certain applications to be monitored
- for the entire day, or for a specified time period

Getting there: Messaging → Security Administration → Application Builder settings



CallPilot Manager - Security Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://cplab230a/cpmgr/msgadmin/security/secadmin.asp
Go Links
Done
Local intranet

Application Builder

Monitor thru-dials for Application Builder applications with associated SDNs □

Monitoring Period (Eastern Time):

From: 00 hh 00 mm

To: 00 hh 00 mm

Note: To display links to all Security Administration procedures, scroll to the bottom of the page and click the Help button.

Looking up procedures in CallPilot Manager online Help

Find procedures for monitoring thru-dialing activity via custom applications by looking up **monitoring** in the Index.

Chapter 10

Configuring mailbox security

In this chapter

Recommendations and guidelines

Introduction

When you set up your CallPilot system, address the following issues:

- Unused mailboxes and inadequate mailbox access controls make it easy for hackers to use your system.
- Mailboxes provide access to features and services using the thru-dial function. Your organization is charged for some of these services on a per-use basis.

Issues and recommendations

Issue	Recommendations
Hackers often use corporate systems to pay for pay-per-minute services, which are accessed via a 9xx access code.	Apply a global RPL to prevent all calls to pay-per-minute services.
Mailbox owners often delay changing their default passwords, which makes it is easier for hackers to gain access to a new mailbox.	Change the password prefix for new mailboxes regularly. Change the default password prefix regularly and include the password prefix in data files used to add groups of mailboxes.

Issue	Recommendations
Hackers look for signs that a mailbox is unused.	Nortel Networks recommends that you take the following actions: ■ Delete unused mailboxes to keep hackers out of your system. ■ Ensure that all mailboxes have recorded spoken names (personal verifications). ■ Ensure that all personal verifications specify the mailbox owner’s name or title, instead of a message such as “The person at extension 8522 is not available to take your call.” See the online Help topics “Confirming the use of a personal verification” and “Providing a personalized greeting for a mailbox.” ■ Ensure that aged messages are automatically deleted from mailboxes. ■ When you create new mailboxes prior to immediate use, defer access to the new mailboxes. **Note:** See the online Help book “Monitoring suspicious activity.”

Issue	Recommendations
Mailbox owners often repeat favorite passwords and choose passwords that are easy to hack.	Educate mailbox owners about how to create secure passwords to increase system security. Nortel Networks recommends that you take the following actions: ■ Specify a minimum password length of eight characters. ■ Force mailbox owners to change their passwords regularly as a good security practice. **Default:** Mailbox owners must change their passwords every 90 days. ■ Play a warning message a few days before mailbox owners’ passwords expire so that they can change the password before it expires. **Default:** Five days. The warning message plays once each day until the password is changed. ■ Ensure that mailbox owners change their passwords to new passwords, rather than entering the same passwords. **Default:** Mailbox owners must enter five new passwords before they can reuse an old password. **Note:** If these defaults do not suit the needs of your organization, see the online Help topic “Changing global mailbox password options.”

Issues and recommendations

Issue	Recommendations
Hackers often use corporate systems to pay for pay-per-minute services, which are accessed via a 9xx access code.	Apply a global RPL to prevent all calls to pay-per-minute services.
Mailbox owners often delay changing their default passwords, which makes it is easier for hackers to gain access to a new mailbox.	Change the password prefix for new mailbox owners regularly. Change the default password prefix regularly and include the password prefix in data files used to add groups of mailbox owners.
Hackers look for signs that a mailbox is unused.	Nortel Networks recommends that you take the following actions: ▪ Delete unused mailboxes to keep hackers out of your system. ▪ Ensure that all mailboxes have recorded spoken names (personal verifications). ▪ Ensure that all personal verifications specify the mailbox owner’s name or title, instead of a message such as “The person at extension 8522 is not available to take your call.” See Confirming the use of a personal verification and Providing a personalized greeting for a mailbox. ▪ Ensure that aged messages are automatically deleted from mailboxes. **Note:** See the online Help book “Monitoring suspicious activity.”

Issue	Recommendations
Mailbox owners often repeat favorite passwords and choose passwords that are easy to hack.	Educate mailbox owners about how to create secure passwords to increase system security. Nortel Networks recommends that you take the following actions: ■ Specify a minimum password length of eight characters. ■ Force mailbox owners to change their passwords regularly as a good security practice. **Default:** Mailbox owners must change their passwords every 90 days. ■ Play a warning message a few days before mailbox owners' passwords expire so that they can change the password before it expires. **Default:** Five days. The warning message plays once each day until the password is changed. ■ Ensure that mailbox owners change their passwords to new passwords, rather than entering the same passwords. **Default:** Mailbox owners must enter five new passwords before they can reuse an old password. **Note:** If these defaults do not suit the needs of your organization, see the online Help topic "Changing global mailbox password options."

Guidelines for creating secure mailbox passwords

Mailbox owners are often unaware of password security risks and how to address them.

Inform mailbox owners about the security risks involved and why these measures are important.

The following guidelines can help mailbox owners create better passwords.

- Do not use obvious dates, names, and words (such as favorite hobbies, food, and so on).
- Use phonetic versions of meaningful words that are easy to remember. Examples: whyzkrak, phabuluss
- Use numbers in place of some letters. These are hard for password-cracking programs to match. Examples: 4ainbow, 8ookworm, pu22led
- Use combinations of words that result in non-words. Examples: apecar, teaflower

Controlling access to mailboxes

Introduction

Define mailbox logon requirements for all system users. Enable and configure security options that control external logons and limit the number of unsuccessful logon attempts.

Mailbox access control default values shipped with CallPilot

Access control	Shipped default value
Number of unsuccessful logon attempts that can be made on a mailbox before it is disabled. **Note:** The administrator must use CallPilot Manager tore-enable the mailbox before it can be accessed again.	9
Number of unsuccessful logon attempts a user can make before a mailbox session is terminated	3 **Note:** For users logging into IMAP client types (for example, by using desktop messaging), the invalid logon count is increased by 2.

Looking up procedures in CallPilot Manager online Help

Find procedures for changing mailbox access control default values by looking up **mailbox access** in the CallPilot Manager online Help Index.

Changing global mailbox password options

Introduction

If the mailbox password defaults shipped with CallPilot do not adequately address the security needs of your organization, change them.

The default password

The default password consists of the password prefix plus the mailbox number. It is truncated at 16 characters whenever the mailbox number exceeds 14 characters.

The default password is in effect whenever

- new mailboxes or administrators are added to the CallPilot database
- after a password is reset

Preventing administrators from being locked out of CallPilot Manager

Administrators can be locked out of CallPilot Manager if they (or someone else) tries to log on with the wrong password too many times. You can minimize the risk associated with this type of denial of service attack.

To avoid manually resetting passwords whenever this happens, you can configure CallPilot Manager to automatically re-enable disabled administrator passwords after the configured length of time.

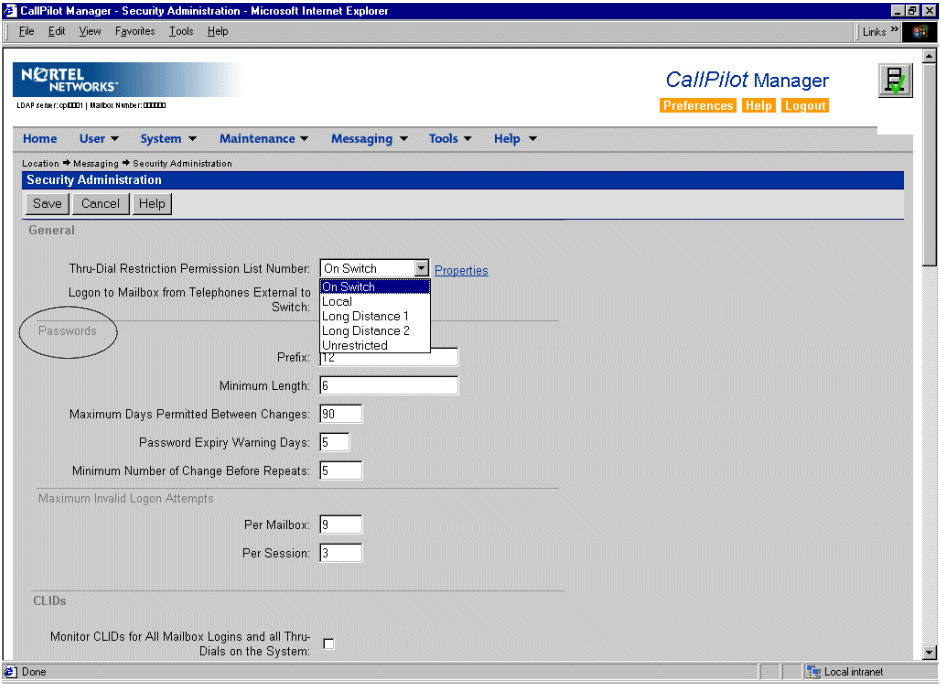
Mailbox password default values shipped with CallPilot

Setting	Shipped default value
Password prefix	12
Minimum length of password	6 characters
Maximum days permitted between changes	90 days
Number of days before password expiry that the mailbox owner receives a warning	5 days
Number of different passwords that mailbox owners must create before recycling an old password	5 passwords

See also

- “Issues and recommendations” on page 245
- “Guidelines for creating secure mailbox passwords” on page 250

Getting there: Messaging → Security Administration → Passwords settings


CallPilot Manager - Security Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
NORTEL NETWORKS
LDAP server: cp□□□1 | Mailbox Number: □□□□□□
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location → Messaging → Security Administration
Security Administration
Save Cancel Help
Properties
On Switch
Local
Long Distance 1
Long Distance 2
Unrestricted
Done
Local intranet

General

Thru-Dial Restriction Permission List Number: On Switch

Logon to Mailbox from Telephones External to Switch:

Passwords

Prefix: 12

Minimum Length: 6

Maximum Days Permitted Between Changes: 90

Password Expiry Warning Days: 5

Minimum Number of Change Before Repeats: 5

Maximum Invalid Logon Attempts

Per Mailbox: 9

Per Session: 3

CLIDs

Monitor CLIDs for All Mailbox Logins and all Thru-Dials on the System: □

Note: To display links to all Security Administration procedures, click the gray Help button.

Looking up procedures in CallPilot Manager online Help

Find procedures for changing mailbox password default values by looking up **mailbox passwords** in the CallPilot Manager online Help Index.

Ensuring the use of a personal verification

Introduction

Hackers look for signs that a mailbox is unused. Nortel Networks recommends that you ensure that all mailboxes have a personal verification recorded for it.

To reduce the administrative burden of recording personal verifications, do at least one of the following:

- Ensure that mailbox owners can record their own.
- Permit another mailbox owner to record personal verifications.

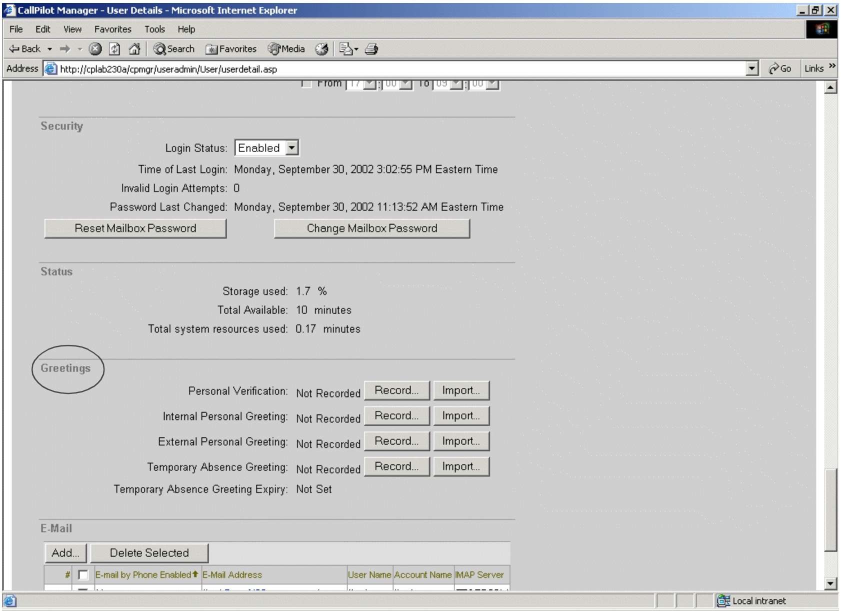
You might need to provide a personalized greeting for a mailbox in either of the following situations:

- You are configuring a special-purpose mailbox.
- You must protect the mailbox from hackers.

See also

- “Issues and recommendations” on page 248
- The CallPilot Manager online Help topic “Setting call answering options for mailbox class members.”

Getting there: User → User Search → User Detail page → Greetings settings


CallPilot Manager - User Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://cplab230a/cpmgr/useradmin/User/userdetail.asp
Go Links
From 17 : 00 To 09 : 00
Reset Mailbox Password
Change Mailbox Password
Record... Import...
Add...
Delete Selected
Local intranet

Security

Login Status: Enabled

Time of Last Login: Monday, September 30, 2002 3:02:55 PM Eastern Time

Invalid Login Attempts: 0

Password Last Changed: Monday, September 30, 2002 11:13:52 AM Eastern Time

Status

Storage used: 1.7 %

Total Available: 10 minutes

Total system resources used: 0.17 minutes

Greetings

Personal Verification: Not Recorded

Internal Personal Greeting: Not Recorded

External Personal Greeting: Not Recorded

Temporary Absence Greeting: Not Recorded

Temporary Absence Greeting Expiry: Not Set

E-Mail

#	☐	E-mail by Phone Enabled	E-Mail Address	User Name	Account Name	IMAP Server

Note: To display links to all User Administration procedures, scroll to the bottom of the page and click the Help button.

Looking up procedures in CallPilot Manager online Help

Find procedures for confirming and providing mailbox personal verifications by looking up **personal verifications** in the CallPilot Manager online Help Index.

Chapter 11

Maintaining restriction permission lists

In this chapter

Overview

Introduction

Certain services and custom applications are capable of using the thru-dial process to place calls outside your system onto the public network. This means they can be used to place long-distance calls that incur toll charges.

Use of restriction permission lists (RPLs) ensures that your organization does not incur unauthorized toll charges.

Each RPL consists of two lists:

- restriction code list
- permission code list

Restriction permission lists

A restriction permission list (RPL) limits the DNs that can be connected to by the thru-dial process.

To adequately secure the CallPilot unified messaging system, RPLs must be applied to each of the following:

- the entire system (the global RPL)
- a mailbox owner group (mailbox class RPLs)
- an individual application or service (application-specific RPLs)

Restriction codes

Restriction codes specify the beginning of a dialed number to which any call is blocked.

For example, if 21 is a restriction code in the Local RPL, and a number that begins with 21 (such as 213-3333) is dialed, the call is blocked.

Permission codes

A permission code is an exception to the corresponding restriction code.

For example, if 21 is a restriction code in the Local RPL, and a number that begins with 21 (such as 213-3333) is dialed, the call is blocked. However, if the Local RPL also includes the permission code 213, a call to 213-3333 is permitted.

Required RPL maintenance tasks

After a CallPilot system is installed, you must

- Customize the On Switch RPL.
- Customize the Local RPL.
- Customize the Long Distance 1 RPL to permit domestic long distance calls.
- Customize the Long Distance 2 RPL to permit international long distance calls.
- Define the global restrictions and permissions for off-switch dialing.
- Apply RPLs to thru-dial features used by mailbox class members.
- Apply a callback handling RPL to any custom applications.

Creating and deleting RPLs

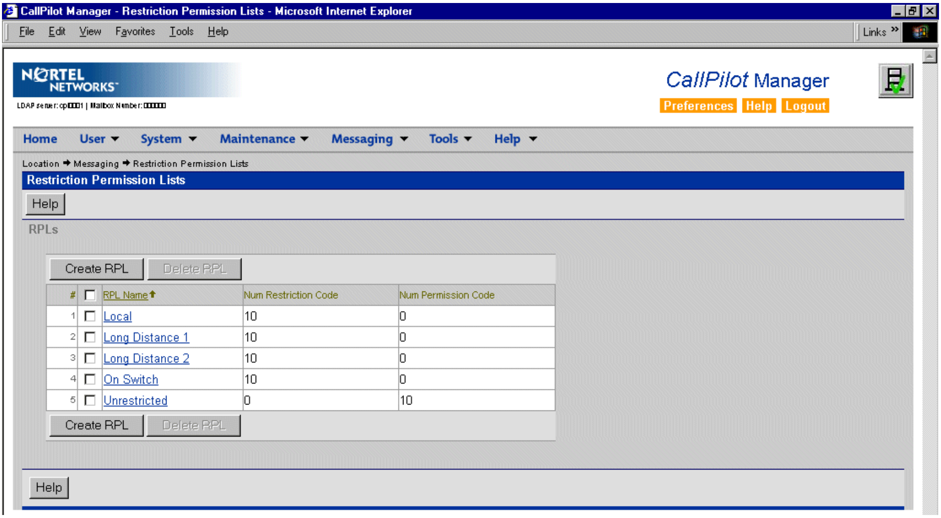
There are four supplied RPLs on newly installed systems. Initially, the restriction codes for these lists are digits 0–9 so that no off-switch dialing is permitted.

For some organizations, these four lists are sufficient. Organizations that have more complex requirements need special-purpose RPLs. CallPilot can store up to 200 RPLs.

Whenever an RPL that you create becomes obsolete, delete it.

Note: You cannot delete a supplied RPL.

Getting there: Messaging → Restriction Permission Lists



CallPilot Manager - Restriction Permission Lists - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Help
Create RPL Delete RPL

Location → Messaging → Restriction Permission Lists

Restriction Permission Lists

RPLs

#	□	RPL Name	Num Restriction Code	Num Permission Code
1	□	Local	10	0
2	□	Long Distance 1	10	0
3	□	Long Distance 2	10	0
4	□	On Switch	10	0
5	□	Unrestricted	0	10

To display the help topic “Maintaining Restriction Permission Lists,” click the gray Help button.

Looking up procedures in CallPilot Manager online Help

Find procedures for maintaining, creating, and deleting RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Determining the need to customize and create RPLs

Introduction

The following processes are not CallPilot Manager tasks. They are administrative processes that help you determine whether you must create special-purpose RPLs.

Creating and customizing RPLs that govern external Call Sender

If a mailbox is compromised, a hacker can listen to messages and use the Call Sender feature to place a call to the message sender.

To prevent unwanted charges without unnecessary restriction of legitimate chargeable calls:

1. Use CallPilot Manager Advanced Search to list the mailbox classes that allow external Call Sender.
2. Determine which mailbox classes should permit mailbox owners to place international long distance calls with no special restriction. Ensure that the Long Distance 2 RPL is customized appropriately.
3. Of the remaining mailbox classes, determine which should permit mailbox owners to thru-dial to domestic long distance DNs with no special restriction. Ensure that the Long Distance 1 RPL is customized appropriately.
4. Of the remaining mailbox classes, determine which should permit mailbox owners to thru-dial to local off-switch DNs with no special restriction. Ensure that the Local RPL is customized appropriately.
5. If there are any mailbox classes left, determine if there are any which should permit off-switch dialing of any kind.
6. If so, list each special restrictions required and create one or more RPLs that block only the restricted calls.

Creating and customizing RPLs that govern the revert DN

If a mailbox is compromised, a hacker can define the number of a long distance carrier as the mailbox owner’s revert DN.

To prevent unwanted charges without unnecessary restriction of legitimate chargeable calls:

1. Use CallPilot Manager Advanced Search to list the mailbox classes that allow mailbox class owners to specify an off-switch revert DN.
2. Determine which mailbox classes, if any, should permit mailbox owners to specify an international long distance number as the revert DN, with no special restriction.
3. Ensure that the Long Distance 2 RPL is customized appropriately.
4. Of the remaining mailbox classes, determine which should permit mailbox owners to specify a domestic long distance number as the revert DN, with no special restriction.
5. Ensure that the Long Distance 1 RPL is customized appropriately.
6. Of the remaining mailbox classes, determine which should permit mailbox owners to specify a local off-switch number as the revert DN, with no special restriction.
7. Ensure that the Local RPL is customized appropriately.
8. If there are any mailbox classes left, determine if there are any which should permit mailbox class members to specify an off-switch number of any kind as the revert DN.
9. If so, list each special restrictions required and create one or more RPLs that block only the restricted calls.

Creating and customizing AMIS Open Networking RPLs

If the CallPilot system has AMIS Open Networking installed, mailbox owners can compose and send messages to mailboxes on other messaging systems on the open (public) network. This openness allows hackers established on your messaging systems to charge their costs to your system.

To prevent unwanted charges without unnecessary restriction of legitimate chargeable calls:

1. Use CallPilot Manager Advanced Search to list the mailbox classes to allow mailbox class owners to send messages over the public network.
2. Determine which mailbox classes, if any, should permit mailbox owners to send messages to an international long distance number, with no special restriction. Ensure that the Long Distance 2 RPL is customized appropriately.
3. Of the remaining mailbox classes, determine which should permit mailbox owners to send messages to a domestic long distance number, with no special restriction. Ensure that the Long Distance 1 RPL is customized appropriately.
4. Of the remaining mailbox classes, determine which should permit mailbox owners to send messages to a local off-switch number, with no special restriction. Ensure that the Local RPL is customized appropriately.
5. If there are any mailbox classes left, determine if there are any which should permit mailbox class members to send messages to an off-switch number of any kind.
6. If so, list each special restrictions required and create one or more RPLs that block only the restricted calls.

See also

“Creating and using a set of search criteria” on page 286

Customizing RPLs

Introduction

This topic provides some recommendations for customizing restriction permission lists (RPLs) to secure the system while thru-dial features are used.

You can restrict calls by international code, area code, or local exchange code by overlapping restriction and permission codes in the same RPL.

Example of overlapping restriction and permission codes in an RPL

A Long Distance RPL must

- prevent mailbox owners from dialing out to a 900 area code
- permit use of the dialing prefix 9, as well as local calls to a 9xx exchange and on-switch calls to extensions beginning with 9

The RPL must include the following:

- Restriction Code: 91900 (assuming that the caller must dial 1 to access a long-distance switch)
- Permission code: 9

Supplied RPLs

For many organizations, the four supplied RPLs, once they are customized appropriately, can be applied to give each thru-dial feature the appropriate level of protection for each mailbox class.

CallPilot supplies

- On Switch RPL
- Local RPL
- Long Distance 1 RPL
- Long Distance 2 RPL

Customizing supplied RPLs

There are four supplied RPLs on newly installed systems. Initially, the restriction codes for these lists are digits 0–9, with no permission codes. This means that each process requiring the thru-dial function fails.

The RPLs page lists, for each RPL, the number of restriction and permission codes defined. By default, each supplied RPL has 10 restriction codes and no permission codes. You can use these summations to determine, at a glance, whether RPLs have been customized.

See also

- “Customizing the On Switch RPL to enable thru-dialing to other on-switch DNs” on page 267

Guidelines for customizing the global RPL

The global RPL governs the call answering, express voice messaging, and thru-dial sessions on the system.

To restrict these features from dialing out to the public network

- Customize the On Switch RPL to prevent off-switch dialing.
- Ensure that the On Switch RPL is specified as the global RPL.

Guidelines for customizing mailbox class RPLs

Plan mailbox classes and user creation templates, and apply each mailbox class RPL to block calls that would result in unwanted charges.

You may need special-purpose RPLs features such as the following:

- external Call Sender
- automated attendant services
- AMIS Open Networking

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing and applying RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Customizing the On Switch RPL to enable thru-dialing to other on-switch DNs

Introduction

Customize the On Switch RPL to permit thru-dialing to other on-switch numbers. Do not permit any off-switch numbers, including local numbers. Apply this RPL to features when maximum security is required.

ATTENTION

When you modify an RPL, the modifications automatically apply to all features to which the RPL is assigned.

Note: For most systems, all restriction codes can be removed.

Default global RPL

The On Switch RPL is the default global RPL.

ATTENTION

If you do not customize the On Switch RPL:

- Mailbox owners cannot successfully thru-dial to any DN while logged on to their mailboxes.
- Mailbox callers cannot thru-dial to any DN during a call answering or express voice messaging session.

Getting there

Messaging → Restriction Permission Lists → On Switch RPL

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Customizing the Local RPL to enable off-switch dialing

ATTENTION

When you modify an RPL, the modifications automatically apply to all features to which the RPL is assigned.

Introduction

Customize the Local RPL so that it allows both on-switch and local numbers to be called, but blocks domestic and international long distance calls. This RPL provides a degree of security since the only off-switch numbers allowed are local.

ATTENTION

The Local RPL is the default applied to each Voice Messaging feature in all supplied mailbox classes. If you do not customize this RPL, thru-dialing will fail, for each mailbox class member, to the following DNs:

- revert DN
- callback DN
- MWI DN

Getting there Messaging → Restriction Permission Lists → Local RPL

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Customizing the Long Distance 1 RPL to enable domestic long distance calls

ATTENTION

When you modify an RPL, the modifications automatically apply to all features to which the RPL is assigned.

Introduction

Customize the Long Distance 1 RPL to permit CallPilot to call domestic long distance.

ATTENTION

Be cautious about the dialing codes you permit, and be careful about the features to which you apply this less secure list. This procedure includes a step to prevent thru-dialing to pay-per-use services.

Getting there Messaging → Restriction Permission Lists → Long Distance 1 RPL

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Customizing the Long Distance 2 RPL to enable international long distance calls

ATTENTION

When you modify an RPL, the modifications automatically apply to all features to which the RPL is assigned.

Introduction

Customize the Long Distance 2 RPL to enable CallPilot to call international numbers.

ATTENTION

Be cautious about the dialing codes you permit, and be careful about the features to which you apply this less secure list. This procedure includes a step to prevent thru-dialing to pay-per-use services.

Getting there Messaging → Restriction Permission Lists → Long Distance 2 RPL

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Applying RPLs

Introduction

RPLs must be applied to each of the following:

- the entire system (the global RPL)
- a mailbox class (a mailbox class RPL)
- an individual application or service (an application-specific RPL)

Note: You can also create special-purpose RPLs. See “Determining the need to customize and create RPLs” on page 261.

Guidelines for selecting the global RPL

The global RPL governs the call answering, express voice messaging, and mailbox thru-dial sessions of all mailboxes on the system.

Select an RPL (such as the On Switch RPL) that allows mailbox callers to dial out to internal extensions only.

You can apply less restrictive rules for mailbox owners than for mailbox callers by applying a different mailbox class RPL to the Outdialing and Thru-dial feature in each mailbox class.

Guidelines for selecting mailbox Class RPLs

To give different mailbox class members different outdialing permissions for each outdialing feature, apply RPLs to features in each mailbox class.

Before you apply mailbox class RPLs to outdialing features in a mailbox class:

1. Find the mailbox class members.
2. Consider the calling requirements of the members and the restrictions needed for cost management and system security.

Then

3. For each mailbox class, determine which outdialing features are needed by mailbox owners in that class.
4. For features mailbox owners do not need, ensure all dialing codes are restricted (digits 0–9 should be defined as the restriction codes).
5. Create an RPL that blocks all outdialing by specifying 0 9 as restriction codes and no permission codes. Give the RPL a meaningful name, such as “Block all Outdialing.”
6. For features mailbox owners require, decide on the appropriate dialing restrictions and permissions for each feature. See Guidelines for creating and customizing RPLs for voice messaging features.
7. Move mailbox owners to other mailbox classes as required.

Guidelines for selecting application-specific RPLs

- Create special RPLs for any thru-dial feature or for any application that has Thru-Dial blocks.
- For an application that includes thru-dial or fax callback capability, apply the RPL when you create the Service Directory Number (SDN).

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing and applying RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Defining global restrictions and permissions for off-switch dialing

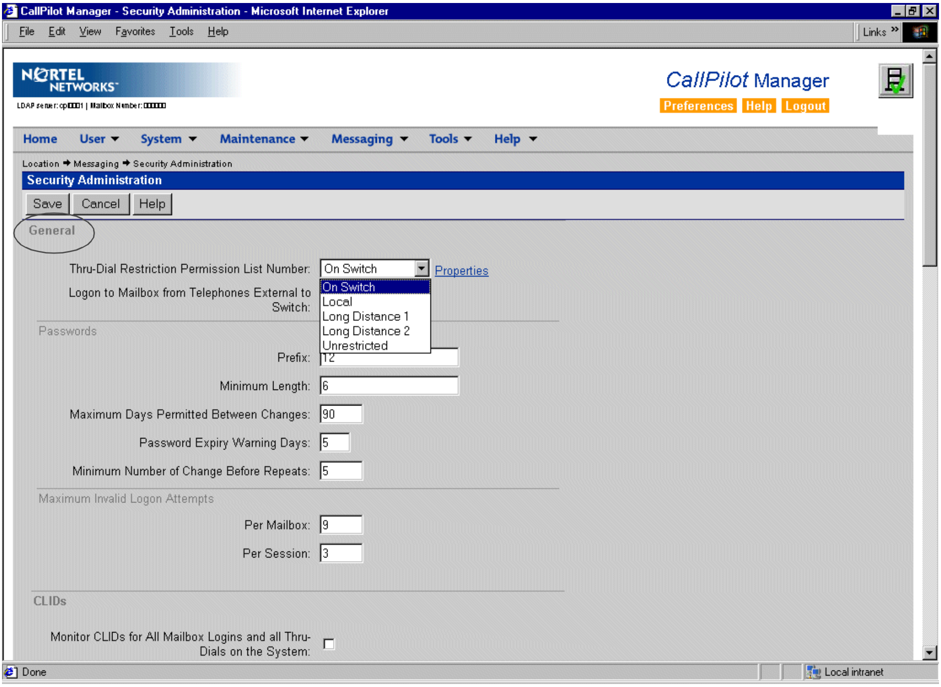
Introduction

The global RPL governs the call answering, express voice messaging, and mailbox thru-dial sessions of all mailbox owners on the system.

ATTENTION

By default, the supplied RPLs prevent all services that use the thru-dial process from connecting to any DN. Customize the supplied RPLs to meet the requirements of your system.

Getting there Messaging → Security Administration


CallPilot Manager - Security Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
NORTEL NETWORKS
LDAP server: cp□□□1 | Mailbox Number: □□□□□□
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Save Cancel Help
Done
Local intranet

Location → Messaging → Security Administration

Security Administration

General

Thru-Dial Restriction Permission List Number: On Switch [Properties]

- On Switch
- Local
- Long Distance 1
- Long Distance 2
- Unrestricted

Logon to Mailbox from Telephones External to Switch:

Passwords

Prefix: 12

Minimum Length: 6

Maximum Days Permitted Between Changes: 90

Password Expiry Warning Days: 5

Minimum Number of Change Before Repeats: 5

Maximum Invalid Logon Attempts

Per Mailbox: 9

Per Session: 3

CLIDs

Monitor CLIDs for All Mailbox Logins and all Thru-Dials on the System: □

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing and applying RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Applying RPLs to thru-dialing services used by mailbox class members

Introduction

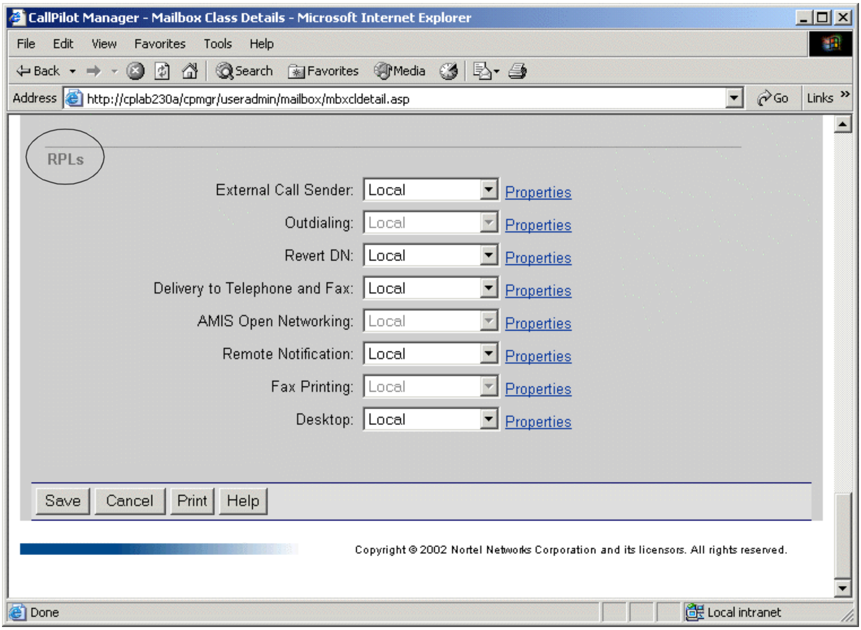
Before you apply RPLs to thru-dialing services for mailbox class members, review the guidelines for doing so and plan any additional RPLs you might need.

By default, the supplied RPLs prevent all governed thru-dialing services from connecting to any DN. Customize the supplied RPLs to meet the requirements of your system. Create new RPLs as circumstances require.

Information you need

- each thru-dialing feature that is available to mailbox class members
- the name of the RPL to be applied to each available feature

Getting there User → Mailbox Classes → Mailbox Class Detail page → RPLs settings



CallPilot Manager - Mailbox Class Details - Microsoft Internet Explorer

Address http://cplab230a/cpmgr/useradmin/mailbox/mbxcldetail.asp

RPLs

External Call Sender:	Local	Properties
Outdialing:	Local	Properties
Revert DN:	Local	Properties
Delivery to Telephone and Fax:	Local	Properties
AMIS Open Networking:	Local	Properties
Remote Notification:	Local	Properties
Fax Printing:	Local	Properties
Desktop:	Local	Properties

Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.

File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Save Cancel Print Help
Done
Local intranet

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing and applying RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Applying a callback handling RPL to a custom application

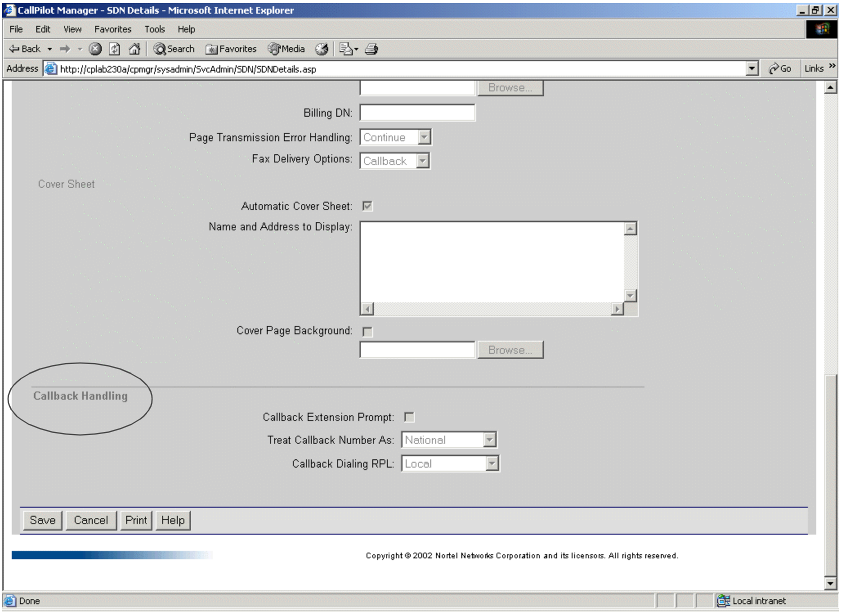
When you apply an RPL to each custom application, consider the calling requirements of the application users and the restrictions needed for cost management and system security.

Note: Before you apply RPLs to applications, review the guidelines for doing so and plan any additional RPLs you might need.

ATTENTION

By default, the supplied RPLs prevent all governed thru-dialing features from connecting to any DN. Customize the supplied RPLs to meet the requirements of your system. Create new RPLs as circumstances require.

Getting there System → Service Directory Number → Service Directory Number page → Callback Handling settings


CallPilot Manager - SDN Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Browse...
Browse...
Save
Cancel
Print
Help
Done
Local intranet

Address http://cplab230a/cpmgr/sysadmin/SvcAdmin/SDN/SDNDetails.asp

Billing DN:

Page Transmission Error Handling: Continue

Fax Delivery Options: Callback

Cover Sheet

Automatic Cover Sheet: ☑

Name and Address to Display:

Cover Page Background: □

Callback Handling

Callback Extension Prompt: □

Treat Callback Number As: National

Callback Dialing RPL: Local

Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing and applying RPLs by looking up **restriction permission lists (RPLs)** in the CallPilot Manager online Help Index.

Part 3

Administering mailboxes

In this part

Chapter 12

Finding mailboxes, administrators, or directory entries

In this chapter

Search methods

Introduction

CallPilot provides the following methods for finding mailboxes, mailbox owners, and specialized administrators:

- Find a specific user by name or mailbox number.
- Define a set of search criteria that describes a group of mailboxes, mailbox owners, or administrators.
- Re-use a saved search.

After search results are displayed you can

- View basic information about the found group of CallPilot mailbox owners or administrators.
- Click the Save Search button to label and save the search criteria.
- Click a Last Name link to display detailed information about a found CallPilot mailbox owner or administrator.
- Click the Delete Selected button to delete the mailbox owners or administrators indicated by a check mark.
- Click the column name box to select or de-select all search results for deletion.
- Click the Add button to add a mailbox owner or administrator that is missing from the group.

Creating and using a set of search criteria

When you must find a group of users that satisfy certain search criteria, an advanced search is appropriate.

You can specify a set of up to three search criteria. You can base search criteria on information that is stored in the CallPilot database.

After you create a search that successfully finds a specific group of users, save it for re-use.

Using a saved search

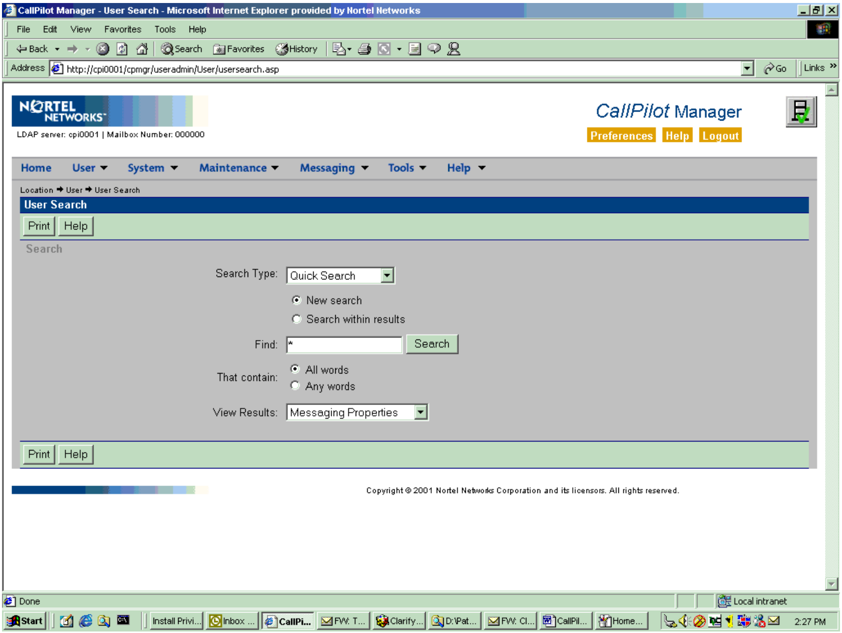
Saved searches are available to any administrative user with access to user search functionality.

For efficient administration, an administrator who is comfortable with defining criteria can create, test and save user searches. Then they are available to any specialized administrator with access to user search functionality.

Changing the scope of a search

- If your search returns a list that is too long to display, narrow down the search.
- If your search does not return all the expected results, broaden the search.

Getting there: User → User Search


CallPilot Manager - User Search - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/useradmin/User/usersearch.asp
Go Links
NORTEL NETWORKS
LDAP server: cpi0001 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location → User → User Search
User Search
Print Help
Search

Search Type: Quick Search

● New search
○ Search within results

Find: * Search

That contain: ● All words ○ Any words

View Results: Messaging Properties

Print Help
Copyright © 2001 Nortel Networks Corporation and its licensors. All rights reserved.
Done
Local intranet
Start Install Privi... Inbox ... CallPi... FW: T... Clarify... D:\Pat... FW: Cl... CallPil... Home...
2:27 PM

Looking up procedures in CallPilot Manager online Help

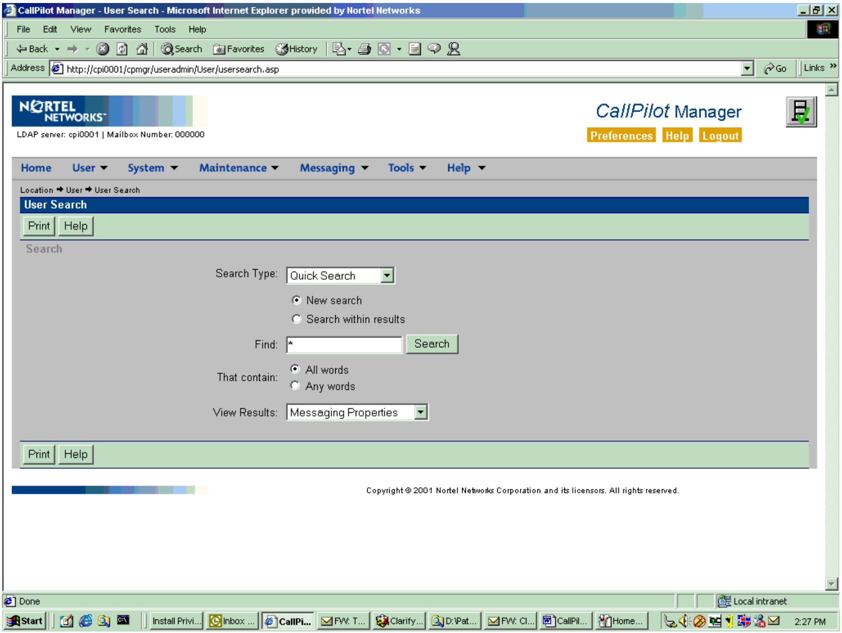
Look up procedures for finding mailbox owners by looking up **mailbox owners** in the Index.

Finding mailbox owners by name or mailbox number

Introduction

When you must find a specific user by name, the quick user search is appropriateAfter you create a search that successfully finds a specific group of users, save it for re-use.

Getting there: User → User Search


CallPilot Manager - User Search - Microsoft Internet Explorer provided by Nortel Networks

Address http://cpi0001/cpmgr/useradmin/User/usersearch.asp

LDAP server: cpi0001 | Mailbox Number: 000000

Location → User → User Search

User Search

Search

Search Type: Quick Search

● New search
○ Search within results

Find: *

That contain: ● All words ○ Any words

View Results: Messaging Properties

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

File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Print Help
Search
Print Help
Done
Local intranet
Start Install Privi... Inbox ... CallPi... FW: T... Clarify... D:\Pat... FW: Cl... CallPil... Home...
2:27 PM

Looking up procedures in CallPilot Manager online Help

Look up procedures for finding mailbox owners by looking up **mailbox owners** in the Index.

Creating and using a set of search criteria

Introduction

When you must find a group of users that satisfy certain search criteria, an advanced search is appropriate.

Recommendations

- After you create a search that successfully finds a specific group of users, use the Save button to save it for re-use.
- An administrator who is comfortable with defining criteria can create, test and save user searches. Then they are available to any full administrator or specialized administrator.

Search criteria

You can define up to three search criteria based on user and mailbox properties stored in the CallPilot database.

For each criteria, specify the following:

- the data element on which to base the criterion (for example, mailbox number)
- the operator that describes the relationship of the data element to the stored values for that data element (for example, EQUAL TO, NOT EQUAL TO, GREATER THAN, LESS THAN)
- the value or values to use for comparison (for example, 3346, 3*, or P)

After you define all search criteria, you can specify whether the search must meet all criteria or any one criterion.

See “Examples of search criteria” on page 289.

Specifying the data element

The Search Criteria list provides data elements on which you can base search criteria. To facilitate location of the data element you need, the list is organized into the following groups:

Group label	Description
General	Information about the mailbox owner or administrator, such as Last Name.
Mailbox	Mailbox information, such as number, language, mailbox class, volume on which it is stored.
DNs	Specified DNs, such as extensions, and personal revert DN. Also the Auto logon capability.
Setup	Configured information such as the conditions under which messages are blocked and whether the name can be dialed by external callers.
Greetings	Whether or not personal greetings are recorded.
Fax Options	All Fax Options settings on the User Properties sheet.
Remote Notification	All Remote Notification settings on the User Properties sheet.
Remote Text Notification	Settings related to configuration of remote text notification for the mailbox.
Mailbox Class Capabilities	Settings, such as capability to use a specified installed unified messaging component, in the mailbox class applied to the mailbox.
Mailbox Class RPLs	The dialing restrictions and permissions assigned to the services available to the applied mailbox class, such as AMIS Networking and External Call Sender.

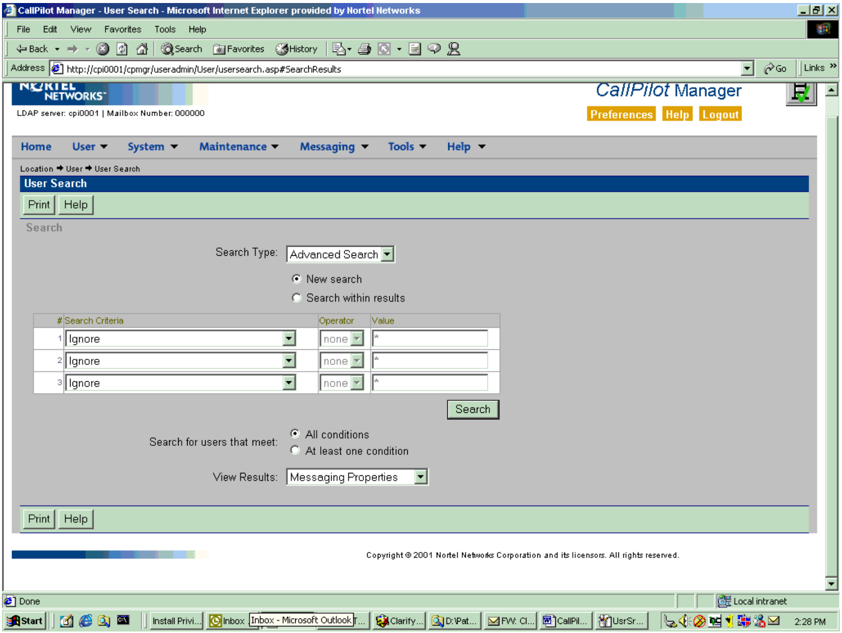
Specifying the operator

After you select a data element from the Search Criteria list, an appropriate list of operators is generated. Select the operator you want to use from the Operator list.

Specifying the value or values to use for comparison

Type the value or values to use for comparison in the Value box. The default value of asterisk (*) returns all stored values described by the relationship between the search data type and the operator.

Getting there: User → User Search → Advanced Search



CallPilot Manager - User Search - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/useradmin/User/usersearch.asp#SearchResults
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location ➔ User ➔ User Search
User Search
Print Help
Search

LDAP server: cpi0001 | Mailbox Number: 000000

Search Type: Advanced Search

● New search
○ Search within results

#	Search Criteria	Operator	Value
1	Ignore	none	*
2	Ignore	none	*
3	Ignore	none	*

Search for users that meet: ● All conditions ○ At least one condition

View Results: Messaging Properties

Print Help
Copyright © 2001 Nortel Networks Corporation and its licensors. All rights reserved.
Done
Local intranet
Start
Install Privi...
Inbox
Inbox - Microsoft Outlook
Clarify...
D:\Pat...
FW: Cl...
CallPil...
UsrSr...
2:28 PM

Looking up procedures in CallPilot Manager online Help

Look up procedures for finding mailbox owners by looking up **mailbox owners** in the Index.

Examples of search criteria

Search Criteria	Search Results
Mailbox Number EQUAL TO 000000	The default full administrator.
Mailbox Number EQUAL TO 8*	A list of all mailbox numbers beginning with 8.
Outcalling Capability EQUAL TO Enabled	A list of all mailboxes with DTT or DTF capabilities.
RN Active on Sunday	A list of all mailboxes with remote notification scheduled on Sunday.
Last Name LESS THAN m	A list of all mailbox owners and administrators with last names beginning A – K.

Chapter 13

Adding and removing mailboxes

In this chapter

Creating new mailboxes or deleting existing ones

Creating new mailboxes

Use the following questions to help you find information.

IF you want to...	THEN see the following procedure
Create only one or a few mailboxes	“Adding mailboxes, one at a time” on page 293
Port mailboxes from a different CallPilot platform	“Adding a group of mailboxes in a single operation” on page 295
Create mailboxes for a new CallPilot system	“Adding a group of mailboxes in a single operation” on page 295

Deleting existing mailboxes

Whenever a mailbox owner leaves the organization, remove the mailbox to prevent misuse by hackers.

Before you can remove mailbox owners, you must search for them, to list them in the Search Results section of the User Administration page.

You can use a Quick Search to find a specific user by name, or you can create an Advanced Search that locates a particular group of users.

Looking up procedures in CallPilot Manager online Help

Find procedures for searching for and removing mailbox owners by looking up **mailbox owners** in the Index.

Adding mailboxes, one at a time

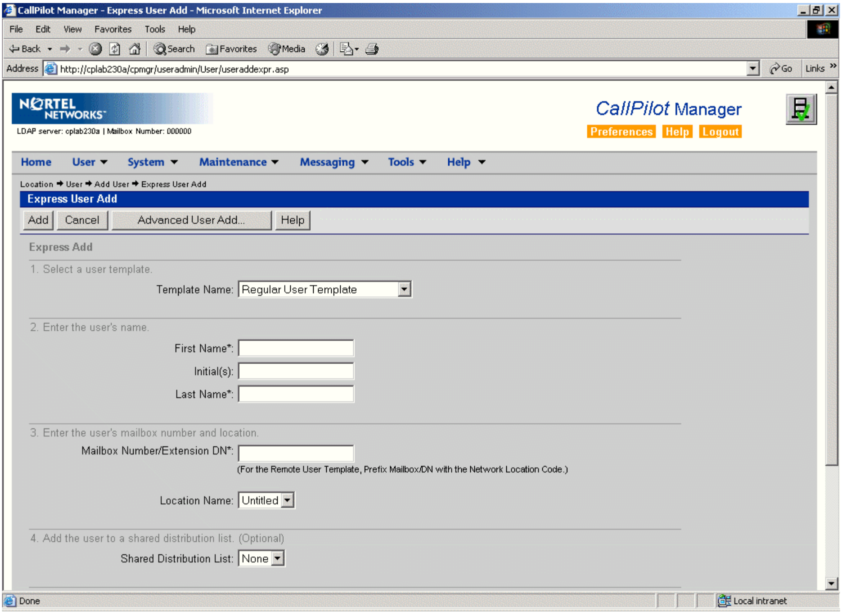
Introduction

CallPilot Manager leads you through the steps required to add a single new mailbox owner to the CallPilot database.

Information you need

- the name of the user creation template
- first and last names of the mailbox owner
- mailbox number (extension DN)
- *optional:* any shared distribution lists to which the mailbox is to be added

Getting there: User → Add User → Express User Add page



CallPilot Manager - Express User Add - Microsoft Internet Explorer

Address http://cplab230a/cpmgr/useradmin/User/useraddexpr.asp

LDAP server: cplab230a | Mailbox Number: 000000

Location → User → Add User → Express User Add

Express User Add

Express Add

1. Select a user template.

Template Name: Regular User Template

2. Enter the user's name.

First Name*:

Initial(s):

Last Name*:

3. Enter the user's mailbox number and location.

Mailbox Number/Extension DN*:

(For the Remote User Template, Prefix Mailbox/DN with the Network Location Code.)

Location Name: Untitled

4. Add the user to a shared distribution list. (Optional)

Shared Distribution List: None

File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Add Cancel Advanced User Add... Help
Done
Local intranet

Looking up procedures in CallPilot Manager online Help

Find procedures for searching for and removing mailbox owners by looking up **mailbox owners** in the Index.

Adding a group of mailboxes in a single operation

Introduction

CallPilot Manager leads you through the steps required to add a group of mailbox owners to the CallPilot database.

Information you need

- the user creation template that is set up for the new mailbox owners
- the name and path of the formatted data input file that contains new mailbox owner information
- If the input data file is an Excel spreadsheet: the name of the worksheet on which the data is stored

The input data file

The input file must include all information that is mandatory for creating a new mailbox.

Required data includes

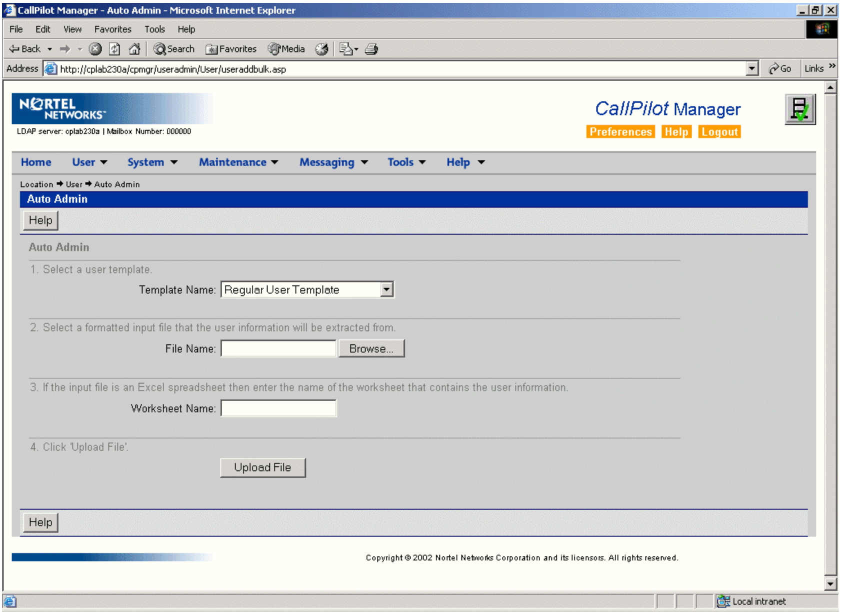
- first and last names of the mailbox owner
- mailbox number (extension DN)

If you are not automatically distributing new mailboxes across volumes, the input file must also include the volume ID.

File format

You can use an Excel worksheet or a text file as a input data file. If you use an Excel worksheet, you will need the name of the worksheet on which the data is stored.

Getting there: User → Auto Admin



CallPilot Manager - Auto Admin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://cplab230a/cpmgr/useradmin/User/useraddbulk.asp
Go Links
NORTEL NETWORKS
LDAP server: cplab230a | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location → User → Auto Admin
Auto Admin
Help

Auto Admin

1. Select a user template.

Template Name: Regular User Template

2. Select a formatted input file that the user information will be extracted from.

File Name: Browse...

3. If the input file is an Excel spreadsheet then enter the name of the worksheet that contains the user information.

Worksheet Name:

4. Click 'Upload File'.

Upload File

Help
Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.
Local intranet

Looking up procedures in CallPilot Manager online Help

Find the procedure for adding mailbox owners by looking up **mailbox owners** in the Index.

Chapter 14

Changing mailbox information

In this chapter

Overview

Introduction

When a mailbox owner changes job functions, update his or her mailbox information as requested.

Looking up procedures in CallPilot Manager online Help

To look up a procedure to	Search the Index for
Change a mailbox owner's personal information.	mailbox owners
Change a mailbox owner's mailbox class.	mailbox owners
Override message blocking for a mailbox.	message blocking
Change the voice gender for E-mail By Phone.	voice gender
Change a mailbox owner’s preferred language.	language
Ensure that mailbox callers are notified of a busy line.	busy line
Set messages to play automatically when the mailbox is accessed.	voice messages
Configure remote notification for a mailbox owner.	remote notification
Change message waiting indication on a mailbox owner's phoneset.	message waiting indication
Add an e-mail account.	e-mail account

See also

“Changing individual mailbox properties” on page 301

Correcting access problems

Introduction

When a mailbox owner cannot access his or her mailbox it might be because of a forgotten password or because the mailbox has been disabled.

If you supervise a team of CallPilot administrators, you might also need to reset CallPilot Manager passwords.

You may also need to enable or disable the ability of a mailbox owner to automatically log on to his or her mailbox from an extension DN.

Resetting a mailbox password

Whenever a mailbox owner forgets a mailbox password, an administrator must reset it.

Re-enabling a mailbox

A mailbox is automatically disabled whenever:

- it has been unused for too long
- there have been too many consecutive unsuccessful attempts to log on.

Enabling or disabling Auto Logon to a mailbox

When Auto Logon is enabled by the mailbox owner, it allows a caller to automatically log on to the mailbox from a DN associated with the mailbox.

For a user to enable or disable Auto Logon to his or her mailbox, the user must be logged on to the mailbox. If no DNs are Autologon-enabled in the user’s profile, the user cannot enable Autologon from a phoneset.

Security feature

To prevent unauthorized access to a mailbox, CallPilot disables Autologon for all DNs whenever an associated DN is added to the user’s DNs list. The enabled DNs remain enabled in the user’s profile, but the user must re-enable Autologon from the phoneset.

Cautions

If a user complains that Autologon is not working when it has been enabled, check for recent changes to the DN list for that user.

Auto Logon should be enabled for phonesets that are in secure locations only.

Looking up procedures in CallPilot Manager online Help

Look up procedures for resetting mailbox or administrator by searching for **passwords** in the Index.

Look up procedures for re-enabling a mailbox by searching for **mailbox access** in the Index.

Look up procedures for enabling and disabling Auto Logon to a mailbox by searching for **mailbox access** in the Index.

Changing individual mailbox properties

Introduction

Use the procedures in this book whenever mailbox owners request changes to their mailbox user properties.

These include

- the personal information associated with the mailbox
- mailbox storage capacity
- the set of mailbox capabilities (mailbox class)
- the E-mail By Phone voice gender
- the mailbox language
- notification of callers whenever the mailbox owner is using a phoneset extension
- automatic playback of new messages whenever the mailbox is accessed
- notification of new or urgent messages to an external (off-switch) DN
- a change in message waiting indication
- overriding the message blocking defaults set for the associated mailbox class

Changing a mailbox owner’s personal information

When a mailbox owner changes job functions, you must update the job title or department.

Changing a mailbox owner’s mailbox class

The mailbox class assigned to the user’s mailbox determines the mailbox capabilities.

When a mailbox owner changes job functions, you might need to assign a more appropriate mailbox class to that user.

Customizing message blocking for a mailbox

The mailbox class assigned to the mailbox owner determines the amount of server space allocated to each mailbox class member. To control resource usage, the mailbox class may specify that when a mailbox is full, new messages are always blocked from the mailbox. Otherwise, messages may never be blocked for mailbox class members.

The user creation template can also determine the circumstances under which messages are blocked for the mailbox owner. When the mailbox owner was added, the template specified when to block incoming messages for all new mailbox owners based on that template.

If the mailbox owner requires different message blocking options than those permitted by the mailbox class, you can override the specification for that mailbox class member only.

Changing the E-mail By Phone voice gender

If mailbox owners can use E-mail By Phone to play their e-mail messages over the phoneset, they may request either a male or female voice.

Changing the mailbox owner’s preferred language

As new languages are installed on the system, users might request that they hear mailbox prompts in a different language.

Note: If the mailbox class specifies it, the mailbox owner’s preferred language is also used for call answering prompts from the mailbox.

Ensuring that mailbox callers are notified of a busy line

If mailbox owners are concerned that callers are informed that the user is occupied on another extension, they may request that you update their mailbox properties.

Setting messages to play automatically when the mailbox is accessed

When a mailbox owner changes job functions, location, or physical circumstances, he or she might request that you set messages to play automatically when the mailbox is accessed. New messages are played first, then old messages.

Configuring remote notification for a mailbox owner

If you want to enable or disable remote notification for an individual mailbox owner but not for an entire group, you can change the remote notification settings for an existing mailbox owner only.

Constraint

You cannot configure remote notification for a mailbox owner unless the mailbox class has remote notification enabled. To find out, locate the Mailbox settings and click Class Details. Ensure that Remote Notification Capability is enabled for the mailbox class.

Mailbox class remote notification settings

You can also use the Mailbox Class Detail page to set remote notification options that are common to mailbox class members.

Whether you enabled remote notification for the individual or it was enabled when the mailbox owner was added to the system, you might also need to specify:

- the target DN and device type for notification messages
- the message type (any new, or only urgent messages) that triggers a notification
- whether notifications are time-stamped in the CallPilot system's or the mailbox owner's time

Configuring remote notification schedules

If the mailbox owner requires notification outside of the usual nine-to-five business hours, and the user's mailbox capabilities do not permit scheduling notifications by using CallPilot phoneset commands, you may need to change the notification schedule.

A mailbox owner may also request that you confirm a notification schedule.

Tip

To avoid configuring each mailbox owner's RN schedule individually, configure the mailbox class so that mailbox owners can schedule remote notifications for themselves via phoneset.

Changing message waiting indication on a mailbox owner's phoneset

If the mailbox owner's position allows too little time to respond each time the message waiting indicator lights up, you can provide support by limiting the types of messages that trigger message waiting indication.

The default is that all new messages trigger message waiting indication.

Adding an e-mail account

Mailbox owners who require access to their e-mail accounts via E-mail By Phone or My CallPilot must have their account information specified in their user properties. For the procedure to define the external e-mail servers that mailbox owners must have to access E-mail By Phone or Web Messaging, see the online Help topic “Managing external e-mail servers.”

Constraints

- You can associate only one mail folder on the server with a particular e-mail address.
- You can assign only one e-mail account at a time for access via E-mail By Phone.

Customizing mailboxes for special purposes

Introduction

Mailbox owners might request special-purpose mailboxes or customizations to their own mailboxes to accommodate special purposes.

Possible requests include

- mailboxes to handle fax deliveries and fax machine overflows
- separate mailboxes when the owners share a phoneset
- separate mailboxes when the owners share an extension
- a mailbox for messages for a group with no single phoneset (such as a help desk)
- a mailbox for occasional guests
- a mailbox where callers can leave suggestions
- automatic playback of new messages whenever the mailbox is accessed
- allowing an assistant to answer a manager’s phoneset when they have separate mailboxes

Setting up mailboxes to handle fax deliveries and fax machine overflows

To handle fax deliveries to owners of mailboxes with no fax capability, configure a fax general delivery mailbox. To handle the overflow from a busy or out-of-paper fax machine, set up a fax overflow mailbox.

Typically, owners of fax overflow mailboxes are administrators who are responsible for distributing incoming messages to the individuals they support. The mailbox owner distributes the messages stored in the fax general delivery mailbox.

- If a fax recipient has a mailbox with fax capability, the mailbox owner can forward the message to the recipient’s mailbox.
- If a fax recipient does not have a fax-capable mailbox, the mailbox owner can print the stored fax and distribute the printed copy to the recipient.

Note: Inform fax general delivery mailbox owners that the order that a mailbox receives faxes might not be reflected in the printing order.

Information you need

- fax general delivery mailbox number
- the fax machine DN (the number published as a group fax number)
- the default printing DN (if Autoprinting is enabled)

Task summary

1. Refer to the Switch Configuration Worksheet (see Part 1 of the *CallPilot Installation and Configuration* binder for your server model) for the following information:
    - the phantom DN to be published as the fax number for a department or organization
    - the phantom DN to use as the fax general delivery mailbox number
2. Ensure the switch is provisioned so that
    - All Busy (Hunt) or No Answer calls to the fax machine are forwarded to the Multimedia Messaging CDN.
    - All calls to the Multimedia Messaging CDN are forwarded unconditionally to the fax machine DN.
    - All calls from the phantom DN are forwarded unconditionally to the fax machine.
    - All messages to the published fax mailbox are forwarded unconditionally to the fax machine designated for the group.
3. Using CallPilot Manager
    - Add the fax general delivery mailbox (a fax-capable mailbox with the phantom DN as the mailbox number) to the CallPilot database.

- Add the fax overflow mailbox (a mailbox, without fax capability, with the fax machine number as the mailbox number) to the CallPilot database.

4. *Optional:* Configure remote notification for all fax general delivery mailbox owners.

Looking up procedures in CallPilot Manager online Help

Look up procedures for configuring special-purpose mailboxes to handle fax deliveries and fax overflows by searching for **fax overflow mailbox** in the Index.

Setting up separate mailboxes for owners who share a phoneset but have their own extensions

In this scenario, several mailbox owners share a phoneset, but each has a separate extension and mailbox.

Example

University teaching assistants share an office that is equipped with one phoneset. Each teaching assistant has his or her own extension on the phoneset. Each extension is associated with a CallPilot mailbox.

	Isabella	Simon
DNs on the switch	3300	3300
Mailbox number	3300	4400
First Extension DN	3300	4400
MWI DN	3300	4400
Callback DN	3300	4400

Note: The MWI By DN feature may be configured on a Meridian 1 or Succession CSE 1000 switch.

Message Waiting Indication

If MWI DNs are configured for all mailboxes associated with the phoneset, the message waiting indicator does not show which mailbox has a new message. To find out if a message is for him or her, the mailbox owner must log on to the mailbox.

Plan how each mailbox owner who shares the phone will be notified of waiting messages.

- You can configure remote text notification for mailbox owners who share a phoneset.
- You can assign message waiting indication to each individual by using the switch MWI By DN feature if both of the following are true:
  - you are using a Meridian 1 or Succession CSE 1000 connectivity
  - X11 software release 24 (or higher) is installed on the switch
- You can configure remote notification of messages if both of the following are true:
  - mailbox owners have remote notification enabled
  - mailbox owners have pagers or cell phones

ATTENTION

Success of the MWI DN configuration depends on switch configuration options that vary from one software version to another. If the MWI DN options that you configure do not work, refer to the Installation and Configuration Guide for your switch.

Switch configuration

Each mailbox owner has the same phoneset DN configured on the switch.

Setting up mailboxes for owners who share a DN

This scenario is often found on a shop floor. There is a single phoneset extension for several workers. Workers can use express voice messaging to leave each other messages.

When no one answers a call to the shared extension, the call is sent to the express voice messaging service. The caller can select a mailbox owner from a voice menu and then record a voice message. When the recipient listens to the message, he or she can use the Call Sender feature to dial the message originator. If both the caller and the message recipient share the phoneset, using the call sender feature will send the call to the express voice messaging SDN.

ATTENTION Plan user groups (mailbox classes and user templates) and assign RPLs to prevent unwanted charges from call sender activity.

Example

If Maryse and Niles share a phoneset extension but have different mailbox numbers, they need the following setup:

	Maryse	**Niles**
DNs on the switch	3300	3300
Mailbox number	25	26
First Extension DN	(blank)	(blank)
MWI DN	3300	3300
Callback DN	3300	3300

Constraint

You cannot configure meaningful message waiting indication for the phoneset.

Information you need

- shared phoneset extension
- each mailbox number

Switch configuration

Each mailbox owner has only the shared extension DN assigned on the switch.

Setting up a mailbox for a group (such as a help desk) with no dedicated phoneset

Where customers call a common phone number for a group (for example, a help desk), the number does not dial a phoneset where the mailbox number matches the first extension DN. Instead, the number dials each phoneset that belongs to a group member.

Example

Pat and Nima both answer calls to the help desk (mailbox 2222).

Pat and Nima also have mailboxes for their personal messages. Pat has mailbox 2345 and Nima has mailbox 2468.

They need the following setup:

	Help desk	Pat	Nima	Optional
DNs on the switch	2222	2345	2468	
Mailbox number	2222	2345	2468	
First Extension DN	2222	2345	2468	
MWI DN	(See note.)	2345	2468	2229
Callback DN	2222	2345	2468	

Note: None, or a DN that is configured on the switch to map to an MWI device for Pat and one for Nima.

Constraint

Any constraints regarding the size of the group are dependent on the switch.

Message Waiting Indication (MWI) issue and workarounds

If MWI DNs are configured for all mailboxes associated with the phoneset, the message waiting indicator does not show which mailbox has a new message.

You can assign message waiting indication to each individual by using the switch MWI By DN feature if both of the following are true:

- you are using a Meridian 1 or Succession CSE 1000 connectivity
- X11 software release 24 (or higher) is installed on the switch

You can configure remote notification of messages if both of the following are true:

- group members have remote notification enabled
- group members have either a shared wireless device or need to be notified off-site of help desk messages.

You can configure remote text notification of waiting messages.

Success of the MWI DN configuration depends on switch configuration options that vary from one software version to another. If the MWI DN options that you configure do not work, refer to the Installation and Configuration Guide for your switch.

Switch configuration

The group is defined as a mailbox owner on the switch as well as the CallPilot server.

Each member of the group is defined as a mailbox owner on the switch as well as the CallPilot server.

Setting up a guest mailbox

In most organizations, short-term contractors and other occasional or one-time visitors need to be able to collect messages from callers. You can set up a guest mailbox that is not associated with a phoneset so these guests can receive and access messages from internal or external callers.

The preferred option of leaving messages is to use the express voice messaging SDN. Messages may also be left using Compose and Send.

Note: If the express voice messaging CDN is not defined, you can use a department assistant's extension. For this information, refer to the Switch Configuration Worksheet (see Part 1 of the *CallPilot Installation and Configuration* binder for your server model).

What you need to know

- the express voice messaging SDN (or a department assistant's extension)
- the mailbox number to use

Switch configuration

The express voice messaging CDN is defined both on the switch and in the CallPilot SDN Table.

Looking up procedures in CallPilot Manager online Help

Look up procedures for customizing mailboxes by searching for **custom mailboxes** in the Index.

Chapter 15

Maintaining shared distribution lists

In this chapter

Overview

Introduction

Create and maintain shared distribution lists (SDLs) to

- optimize your CallPilot resources
- facilitate the use of broadcast messages

CallPilot can store up to 150 SDLs, each containing up to 999 mailboxes.

To be able to use SDLs, a mailbox owner must belong to a mailbox class that provides permission to use shared distribution lists (SDLs).

Benefits of maintaining SDLs

Maintaining a comprehensive list of SDLs optimizes your server’s capacity because it minimizes the need for mailbox owners to create their own personal distribution lists (PDLs).

When mailbox owners create PDLs from their phonesets, those lists are available only to the creator. Each PDL allows the user to send a recorded message to all the mailboxes contained in the list. A mailbox owner can create up to 99 personal distribution lists, each containing a maximum of 200 mailboxes.

Each SDL is one address, regardless of the number of entries on the list. However, each entry on a PDL is one address. For example, an SDL with ten entries is one address, while a PDL with ten entries is ten addresses.

SDLs and multimedia messages

Many mailbox owners with SDL privileges can use SDLs to send both voice and fax messages. You cannot assume that external numbers can receive fax messages. Create separate SDLs for voice and fax messages.

Adding or removing SDL members

Valid SDL members

You can include any CallPilot entity in an shared distribution list (SDL) that has a either a recognizable, unique name or a mailbox number. These include:

- local mailbox owners
- directory entries
- permanent remote mailbox owners

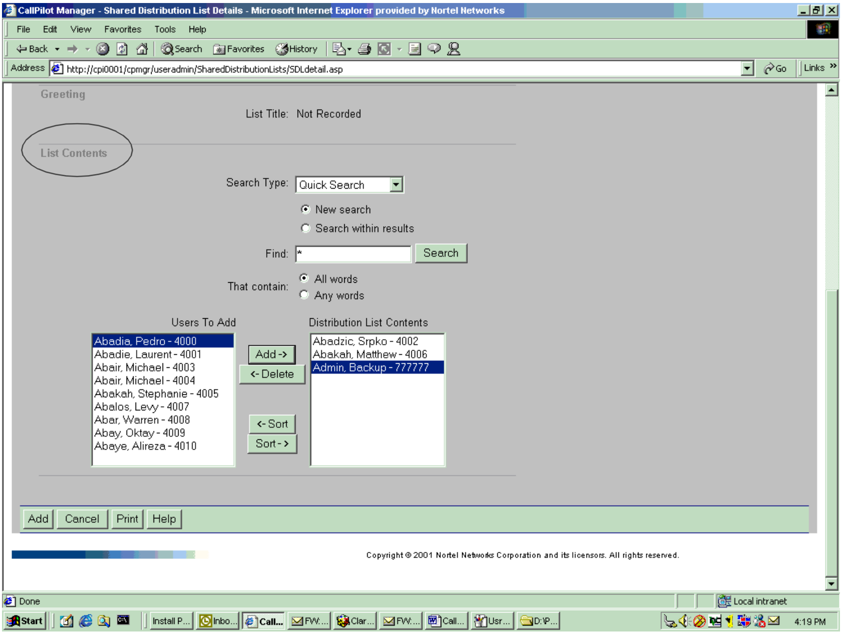
To include users at remote sites in a CallPilot network, you must define them as remote voice users in the local database. To include a remote user site in an SDL, you must define the site and location in your messaging network database.

Constraints

The following types of numbers do not have mailboxes associated with them, so they cannot be included in an SDL:

- remote notification (RN) targets
- non-users who require delivery to telephone (DTT)
- SDL addresses

Getting there: User → Shared Distribution Lists → Shared Distribution List Detail page → List contents settings



CallPilot Manager - Shared Distribution List Details - Microsoft Internet Explorer provided by Nortel Networks

Address http://cpi0001/cpmgr/useradmin/SharedDistributionLists/SDLdetail.asp

Greeting

List Title: Not Recorded

List Contents

Search Type: Quick Search

● New search
○ Search within results

Find: *

That contain: ● All words ○ Any words

Users To Add	Distribution List Contents
Abadia, Pedro - 4000	Abadzic, Srpko - 4002
Abadie, Laurent - 4001	Abakah, Matthew - 4006
Abair, Michael - 4003	Admin, Backup - 777777
Abair, Michael - 4004	
Abakah, Stephanie - 4005	
Abalos, Levy - 4007	
Abar, Warren - 4008	
Abay, Oktay - 4009	
Abaye, Alireza - 4010	

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

File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
Search
Add ->
<- Delete
<- Sort
Sort ->
Add Cancel Print Help
Done
Local intranet
Start Install P... Inbo... Call... FW:... Clar... FW:... Call... Usr... D:\P...
4:19 PM

Looking up procedures in CallPilot Manager online Help

Find procedures for adding or removing SDL members by looking up **SDLs** in the Index.

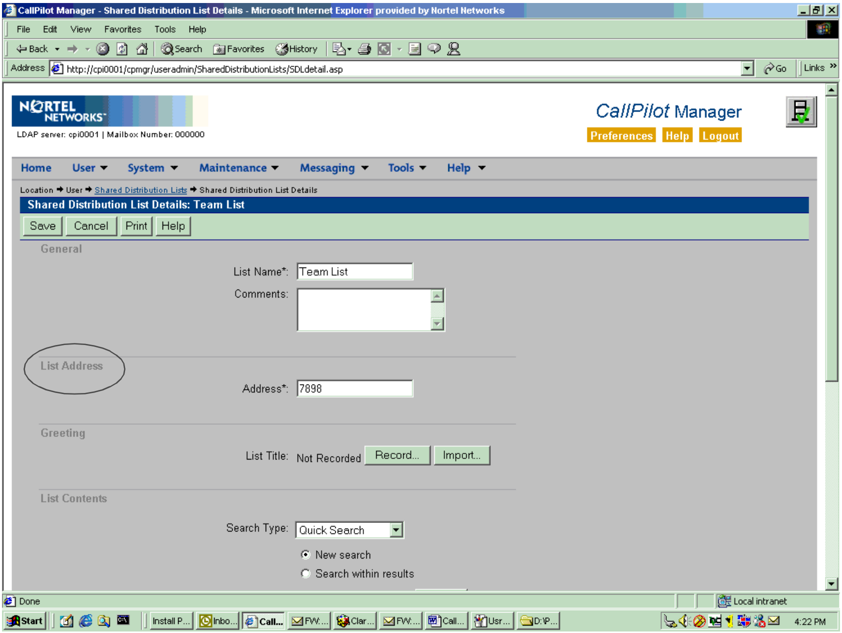
Specifying or changing an SDL address

Restrictions on SDL addresses

The following restrictions are placed on distribution list (SDL) addresses:

- An SDL cannot be assigned an address between 1 and 99. These are reserved for mailbox owners' personal distribution lists (PDLs).
- Each SDL must have a unique address.
- An SDL address must not conflict with any dialing plan prefixes or codes.
- An SDL address cannot be the same as any mailbox number, including the broadcast mailbox number. The default broadcast mailbox number is 5555.
- An SDL address cannot be the same as a directory entry DN. If an SDL number and a directory entry user number are the same, the SDL number takes priority when a list is created.

Getting there: User → Shared Distribution Lists → Shared Distribution List Detail page



CallPilot Manager - Shared Distribution List Details - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/useradmin/SharedDistributionLists/SDLdetail.asp
Go Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Save Cancel Print Help
Record... Import...
Done
Local intranet
Start
4:22 PM

LDAP server: cpi0001 | Mailbox Number: 000000

Location → User → Shared Distribution Lists → Shared Distribution List Details

Shared Distribution List Details: Team List

General

List Name*: Team List

Comments:

List Address

Address*: 7898

Greeting

List Title: Not Recorded

List Contents

Search Type: Quick Search

● New search

○ Search within results

Looking up procedures in CallPilot Manager online Help

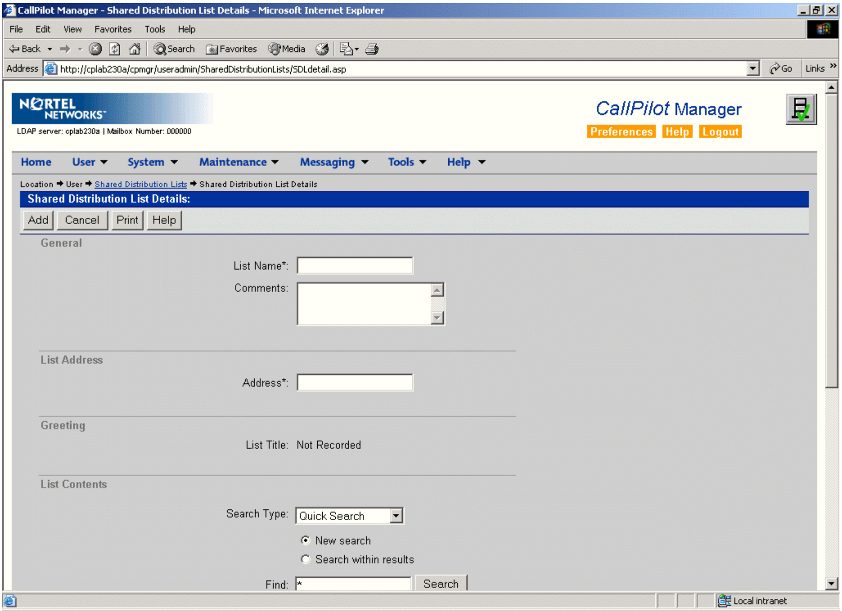
Find procedures for specifying or changing an SDL address by looking up **SDLs** in the Index.

Adding an SDL

Information you need

Before you can create a shared distribution list, you must know the SDL address that specifies the list.

Getting there: User → Shared Distribution Lists → Add



CallPilot Manager - Shared Distribution List Details - Microsoft Internet Explorer

Address http://cplab230a/cpmgr/useradmin/SharedDistributionLists/SDLdetail.asp

LDAP server: cplab230a | Mailbox Number: 000000

Location → User → Shared Distribution Lists → Shared Distribution List Details

Shared Distribution List Details:

General

List Name*:

Comments:

List Address

Address*:

Greeting

List Title: Not Recorded

List Contents

Search Type: Quick Search

● New search

○ Search within results

Find: *

Looking up procedures in CallPilot Manager online Help

Find procedures for adding or removing an SDL by looking up **SDLs** in the CallPilot Manager online Help Index.

Part 4

Managing mailbox creation and privileges

In this part

Chapter 16

User creation templates and mailbox classes

In this chapter

Overview

Introduction

Administrators who manage mailbox creation and privileges support administrators who administer mailboxes and mailbox owners.

If you are creating a team of specialized administrators, consider giving responsibility for maintaining user creation templates and mailbox classes to the same administrator.

How user creation templates differ from mailbox classes

Introduction

User creation templates and mailbox classes are both used to manage mailbox privileges and properties.

	User creation template	Mailbox class
Functionality	Each template provides the default values to be applied to a new group of mailboxes. These values include mailbox capabilities and personal information about mailbox owners such as job title or department.	A mailbox class consists of a set of mailbox and messaging privileges that you can assign to mailbox owners.
Changes	Once you have used the template to add mailboxes to the CallPilot database, you can override default values for an individual mailbox. Any changes made to the template have no effect on mailboxes already based on the template.	Updating a mailbox class automatically updates the mailbox privileges of all members of that mailbox class.

Chapter 17

Using templates to create new mailboxes

In this chapter

Overview

Introduction

CallPilot user creation templates provide a method for you to

- create new mailbox owners efficiently
- document the mailbox properties and user information that were applied to groups of mailbox owners when they were first created

To use this CallPilot feature as it is intended, you must

- maintain a set of user creation templates
- customize the settings for each new group of mailbox owners

You might or might not have to add user creation templates.

Looking up procedures in CallPilot Manager online Help

Find procedures for adding, duplicating, customizing, and deleting templates by looking up **user creation templates** in the CallPilot Manager online Help Index.

Maintaining a set of user creation templates

Introduction

When you maintain a set of user creation templates, you must keep records and delete obsolete templates from the system.

As you maintain these templates, configure the common mailbox privileges required by each group of users. For example, external sales people might require the E-mail by Phone feature, whereas internal sales people can be restricted from using the feature to ensure that the required CallPilot resources are always available to those who need them.

Benefits of using templates

When you configure the settings in a template, those settings appear as defaults for any new user mailbox that you create with that template. You can then fill in the user’s name, mailbox number and password, and make changes to the default feature settings if desired.

The template is a starting point for creating the user. If you create a mailbox owner or other user and then reconfigure the template, this does not affect the settings for the already-created user.

Planning a custom set of templates

CallPilot supplies a basic set of user creation templates. When you first configure your CallPilot system, decide which of the supplied templates you need and then customize each to suit your needs.

You might want to create several versions of a single supplied template. For example, if your organization has different support personnel for each language provided, you might need to create an Internal Sales template, based on the Regular User template, and then use the Internal Sales template as a basis for each Internal Sales (Language) template.

Template documentation

Print a hard copy of the following reports for your records:

- the name of the selected template
- a list of names for all defined templates
- a detailed list of all properties of each template

Looking up procedures in CallPilot Manager online Help

Find procedures for maintaining templates by looking up **user creation templates** in the CallPilot Manager online Help Index.

Creating and deleting user creation templates

Introduction

Create user creation templates to facilitate adding large groups of mailbox owners with a single action.

Before you start creating new templates, see “Maintaining a set of user creation templates” on page 331.

Duplicating templates

To create a new user creation template quickly and easily, duplicate an existing template and rename it. The properties of the existing template are transferred to the new one. You can then customize the settings for a new group of mailboxes.

Deleting templates

As templates become obsolete, delete them.

Looking up procedures in CallPilot Manager online Help

Find procedures for adding, duplicating, customizing, and deleting templates by looking up **user creation templates** in the CallPilot Manager online Help Index.

Customizing settings for new mailboxes

Introduction

To customize settings for a new user group, modify the user creation template to be applied to new mailboxes before you create the mailboxes.

ATTENTION Changes to user creation templates do not affect existing mailboxes.

Template name

Use a template name that uniquely identifies the ongoing purpose of the template. For example, if the template is created to add mailboxes with prompts in a secondary language, ensure that the language is included in the template name.

Comments

Use the Comments box to type information about the user groups to be created using the default settings you are specifying.

Specify information common to all mailboxes

If you know that settings will be unique for different mailboxes, leave them blank in the template.

Looking up procedures in CallPilot Manager online Help

Find procedures for adding, duplicating, customizing, and deleting templates by looking up **user creation templates** in the CallPilot Manager online Help Index.

Choosing a template for customization or duplication

Introduction

When you choose a supplied template for customization or duplication, ensure that it includes all the settings you must use.

CallPilot supplies the following user creation templates.

- Regular User Template
- Basic User Template
- Executive User Template
- Assistant Template
- Administrator Template
- Remote User Template
- Directory Entry User Template
- Admin Only Template
- Fax Buffering Mailbox Template

Different templates have different settings

Some templates have a restricted number of settings. The following tables show which supplied templates have all possible settings, and which do not.

Templates with all possible settings

The following templates include all possible settings:

- Regular User Template
- Basic User Template
- Executive User Template
- Assistant Template
- Administrator Template
- Fax Buffering Mailbox Template

The following table shows the list of all possible template setting groups.

Setting groups	Settings
General	Template Name Comments Title Department
Admin	Administration Type (functions)
Mailbox	Mailbox Class Language Location Name Mailbox File System Volume ID **Note:** You cannot change this volume later. Instead, you must delete the mailbox and re-create it.
DNs	Revert DN
Setup	Short Prompts DTT DTMF confirmation required Auto play Play call answering instruction prompt Auto deletion of invalid PDL addresses Name dialable by external callers Callers notified of busy line TTS Voice Gender Message waiting indication options Block Incoming Messages Block Message Call Handling
Fax Options	Auto printing Print first page only Print separator page Default printing DN

Setting groups	Settings
Remote Notification	Remote Notification On Message Type Device Type Callback Number Days Active Time Period Display Time Values As
Wireless And E-mail Message Waiting Indication	Wireless And E-mail MWI Enabled Notification Device Class Unicode Capable Device Notify For
Security	Logon Status

Templates with a limited number of settings

The following templates include only the necessary settings:

- Admin Only Template
- Remote User Template
- Directory Entry User Template

Looking up procedures in CallPilot Manager online Help

Find procedures for adding, duplicating, customizing, and deleting templates by looking up **user creation templates** in the CallPilot Manager online Help Index.

Chapter 18

Using mailbox classes to manage mailbox privileges

In this chapter

Overview

Introduction

A mailbox class consists of a set of mailbox and messaging capabilities that you can assign only to those mailbox owners who need those capabilities.

Updating a mailbox class automatically updates the mailbox privileges of all mailbox class members.

CallPilot includes supplied mailbox classes to provide you with a starting point to group mailbox owners. You can create custom mailbox classes to suit special needs.

Examples of special-purpose mailbox classes

You can create the following mailbox classes for a small office:

- **General** provides only those mailbox privileges required by the typical mailbox owner.
- **Executive** provides extra storage space for messages as well as message broadcast capability.
- **Sales** provides extra storage space for messages as well as E-mail By Phone capability (so sales people can check e-mail messages from a cell or pay phone).

What mailbox classes govern

Use mailbox classes to specify the following for mailbox class members:

- mailbox storage capacities and other resource usage controls
- call answering options
- message delivery options
- keycoded features they are permitted to use

- dialing restrictions and permissions for CallPilot messaging features and services that use the thru-dial function.

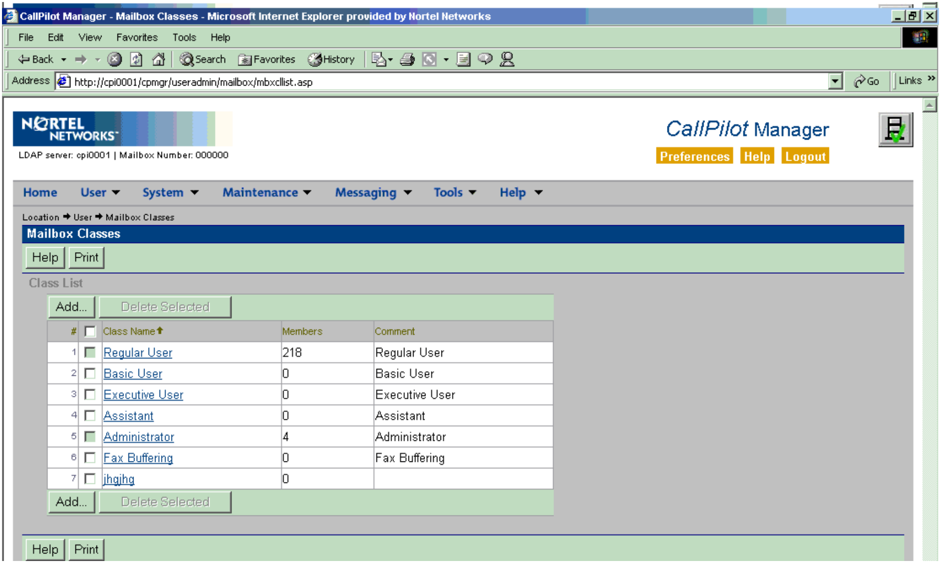
Viewing mailbox privileges for mailbox class members

To view the mailbox privileges configured for a group of mailbox owners, display the mailbox class assigned to the mailbox owner group.

Printing mailbox class information

You can use the Print button on the Mailbox Class Browser page to print a time-stamped list of all configured mailbox classes.

Getting there User > Mailbox Classes


CallPilot Manager - Mailbox Classes - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/useradmin/mailbox/mbxcllist.asp
Go Links
NORTEL NETWORKS
LDAP server: cpi0001 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location User Mailbox Classes
Mailbox Classes
Help Print
Class List
Add... Delete Selected

#	□	Class Name	Members	Comment
1	□	Regular User	218	Regular User
2	□	Basic User	0	Basic User
3	□	Executive User	0	Executive User
4	□	Assistant	0	Assistant
5	□	Administrator	4	Administrator
6	□	Fax Buffering	0	Fax Buffering
7	□	jhgjhg	0	

Add... Delete Selected
Help Print

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring mailbox classes by looking up **mailbox classes** in the CallPilot Manager online Help Index.

Creating and deleting mailbox classes

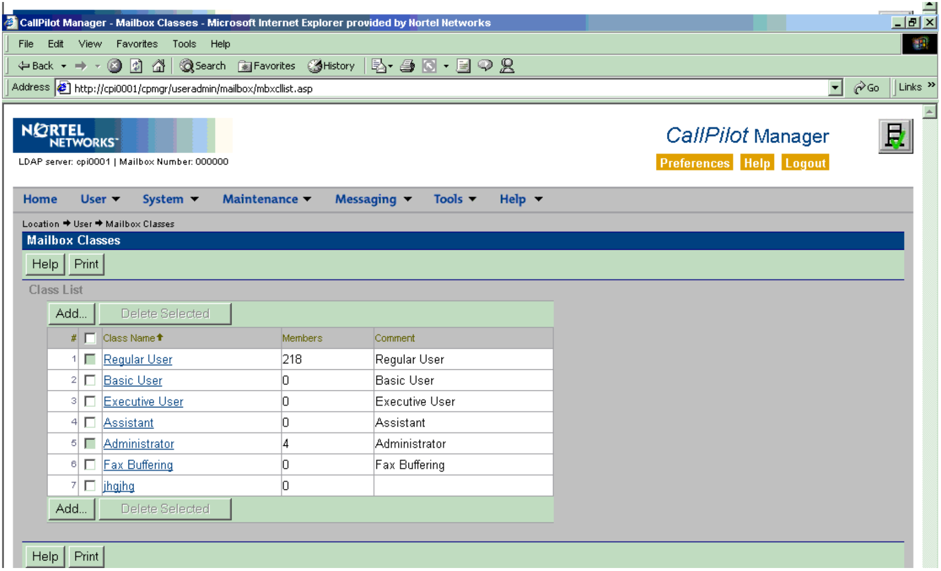
Introduction

The method you choose to create a new mailbox class depends on whether you want it to have properties similar to an existing mailbox class, or whether you want to start with all CallPilot mailbox class defaults.

Constraint

You cannot delete a mailbox class if it has any members.

Getting there User > Mailbox Classes


CallPilot Manager - Mailbox Classes - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/useradmin/mailbox/mbxcllist.asp
Go Links
NORTEL NETWORKS
LDAP server: cpi0001 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location User Mailbox Classes
Mailbox Classes
Help Print
Class List
Add... Delete Selected

#	□	Class Name	Members	Comment
1	□	Regular User	218	Regular User
2	□	Basic User	0	Basic User
3	□	Executive User	0	Executive User
4	□	Assistant	0	Assistant
5	□	Administrator	4	Administrator
6	□	Fax Buffering	0	Fax Buffering
7	□	jhgjhg	0	

Add... Delete Selected
Help Print

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring mailbox classes by looking up **mailbox classes** in the CallPilot Manager online Help Index.

Configuring mailbox classes

Introduction

A mailbox class is a way to define messaging capabilities for a group of mailbox owners. You can change mailbox privileges for a group after the mailbox class has been assigned to mailbox owners. Changes automatically apply to existing members of the modified mailbox class.

Customizing mailbox classes

You might need to customize the supplied mailbox classes before you apply them to user creation templates or to individual mailboxes.

To customize a mailbox class, use either of the following methods as they suit your organization's plans:

- Make basic changes to the supplied template.
- Create new specialized templates by copying the modified basic template and then make specific changes to the specialized templates.

Note: To help you decide how to apply or customize mailbox classes, review the default values for each supplied mailbox class. To find a summary, refer to the CallPilot Manager online Help.

Example of customizing a mailbox class to accommodate a secondary language

If your CallPilot system is multilingual, you might need to create a custom copy of each basic mailbox class for each installed language.

For example, after you make changes that apply to all regular users (regardless of language or other special considerations) to the Regular User mailbox class, create a Regular French mailbox class and, in the Call Answering section of the Mailbox Class Detail page, modify the Language for Callers setting.

Configuration tasks

1. Display the mailbox class properties.
2. Control the amount of resources used by the mailbox.
3. Set call answering options.
4. Set message delivery options.
5. Permit mailbox class members to use keycoded features:
   - To receive and print faxes if the CallPilot system is equipped with fax capability, and mailbox class members require fax-capable mailboxes.
   - To speak CallPilot phoneset commands if the system is equipped with speech activated messaging and the permission justifies the extra resources required.
   - To use a personal computer to access and manage messages if there are enough Desktop Messaging licenses to give the permissions.
   - To listen to e-mail messages over a phoneset if the E-mail by Phone feature is installed and mailbox owners must screen e-mail messages at any given time.
6. Set remote notification privileges for mailbox class members if mailbox class members must configure home phones, cell phones, or pagers to automatically receive message notifications.
7. Control telecom charges by specifying the dialing permissions and restrictions for each feature enabled for mailbox class members.

ATTENTION

All supplied restriction permission lists (RPLs) prevent off-switch dialing. They must be customized before you apply them.

All supplied mailbox classes have features assigned to the Local RPL. You must manually change the RPL assignments to let mailbox users send messages to remote sites.

Permitting use of optional unified messaging components

Introduction

Use mailbox classes to limit use of optional unified messaging components to those mailbox owners who really need them.

Use the Keycoded Features section of each Mailbox Class Detail page to enable the following unified messaging components:

- fax messaging
- speech activated messaging
- desktop and Web messaging
- E-mail by Phone

Permitting mailbox class members to receive and print faxes

If fax capability is not installed on the CallPilot server, the corresponding check box is not included in your mailbox class options.

Note: Fax messaging requires twice the system resources that voice messaging requires.

Permitting mailbox class members to speak CallPilot phoneset commands

If the speech activated messaging capability is not installed on the CallPilot server, the corresponding check box is not included in your mailbox class options.

Controlling resource use

Speech activated messaging requires four times the system resources that voice messaging requires.

Instruct mailbox owners to use speech activated messaging only when DTMF input is not possible or difficult, such as when calling from an external rotary phone or from a cell phone, and not as the normal way to interact with their mailboxes.

Permitting mailbox class members to use a computer to manage messages

When you apply mailbox classes that permit use of a computer or wireless device to manage messages, consider grouping mailbox owners by their workstation capabilities.

The CallPilot system must be keycoded to accommodate all desktop messaging users. The desktop messaging license also permits each desktop messaging user to access My CallPilot.

Permitting mailbox class members to manage their mailboxes from the Web

You can control access to My CallPilot features and configuration options by applying a mailbox class with the required permissions. When choosing which permissions to grant, consider the following dependencies:

- Configuration of some features is only available from My CallPilot. For example, mailbox owners can only set preferences for the Remote Message Waiting Indicator and E-mail by Phone from My CallPilot.
- Some features are easier to use in My CallPilot. For example, you can assign a name and number to a personal distribution list (PDL) in My CallPilot. From the telephone, you can only assign a number to a PDL.
- Mailbox Manager capability controls the availability of specific settings on the CallPilot Features tab in My CallPilot.
    - Message Notification
    - Personal Distribution Lists
    - Change Password
    - Telephone Options

Examples of Web mailbox management permissions

The table below describes two examples of permissions you can assign in the mailbox class.

Permitting mailbox class members to listen to e-mail messages over a phoneset

If the Email-by-Phone capability is not installed on the CallPilot server, the corresponding check box is not included in your mailbox class options.

SSL protection

If your organization requires SSL protection on e-mail messages from all IMAP clients, enable Can Set Up SSL for an IMAP Server.

Configuring Email-by-Phone preferences

The Mailbox Manager Web interface is the only way mailbox owners can configure Email-by-Phone preferences.

part 5

Configuring service defaults

In this part

Chapter 19

Configuring addressing conventions

In this chapter

Specifying off-switch dialing prefixes

Introduction

For off-switch calls, CallPilot requires dialing information to translate a dialed number into a dialable number.

Dialing information consists of

- information required to dial out from the local switch and access a private (ESN) or public network
- information required to distinguish certain area or city codes which are used for either local calls or long distance calls, depending on the destination DN

How dialing prefixes are used

Dialing information is used primarily to translate an external DN for playback to the mailbox owner and the Call Sender feature

How the Call Sender feature uses dialing prefixes

Whenever a mailbox owner presses 9 while playing a message, CallPilot must generate the DN to connect to the calling number.

Whenever the calling number is off-switch, CallPilot uses the configured dialing default prefixes to handle normal dialing situations for local, national, international, and (if they exist) ESN calls.

Example of how CallPilot handles a call initiated by Call Sender

- When a mailbox owner listens to a message delivered by a local call over the public network and then invokes Call Sender to return the call, CallPilot adds the prefix required to place off-switch calls (in North America, this is typically 9).
- When a mailbox owner listens to a message delivered by a call over ESN and then invokes Call Sender to return the call, CallPilot adds the prefix required to place an ESN call (for example, 6).

Dialing translation definitions

CallPilot uses dialing translation definitions to determine how to treat DNs with mixed area or city codes. Mixed area or city codes may be either local or long distance for a location, depending on the exchange code.

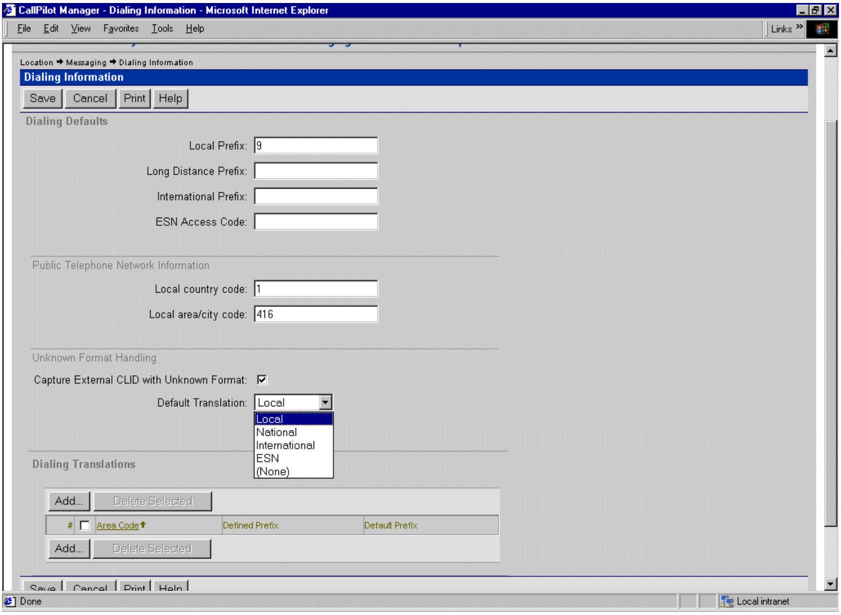
Default translations

CallPilot Manager facilitates configuration of dialing translation definitions by requiring you to specify only the exceptions to the rule. See the examples starting on page 355.

See also

- “Handling mixed area or city codes” on page 355
- “Enabling off-switch calls” on page 366
- CallPilot Manager online Help topic “Specifying off-switch dialing prefixes”

Getting there Messaging → Dialing Information



CallPilot Manager - Dialing Information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Location → Messaging → Dialing Information

Dialing Information

Dialing Defaults

Local Prefix: 9

Long Distance Prefix:

International Prefix:

ESN Access Code:

Public Telephone Network Information

Local country code: 1

Local area/city code: 416

Unknown Format Handling

Capture External CLID with Unknown Format: ☑

Default Translation: Local

Local
National
International
ESN
(None)

Dialing Translations

#	□	Area Code	Defined Prefix	Default Prefix

Add... Delete Selected
Save Cancel Print Help
Done
Local intranet

Handling mixed area or city codes

Introduction

Whether an area code indicates a local or long distance number depends on the calling location. In low-density population areas, a matching area code indicates a local call and a different area code indicates a long distance call. In high-density population areas, a call to an area with a different area code is often treated as a local call because new area codes are introduced to accommodate all the telephone numbers required for area residents.

When to define dialing translations for a mixed area code

When the area code is not sufficient to identify whether a call is local or long distance, the combination of the area code and the local exchange is used to make the distinction. If your CallPilot server is located in a high-density population area use dialing translation definitions to identify the local area code/local exchange combinations.

How dialing translation definitions are used

Dialing translation definitions are used primarily to translate an external DN for playback to the mailbox owner and the Call Sender feature For example, if an Area Code/Exchange Code list is defined as long distance, the message envelope playback includes the prefix 1.

Example: Local and long distance calls with the same area code

Andrei lives in Uxbridge and works in Markham, just north of Toronto. One of Andrei’s major customers is located in Toronto.

Andrei’s location	Telephone number
Home in Uxbridge	905-555-3467
Office in Markham	905-479-9876
Customer in Toronto	416-957-7340

Among these locations, some calls are local calls and some are long distance calls, depending on the origin and destination of the call.

Origin	Destination	Charges	Calling number playback
Toronto customer 416-957-7340	Markham office 905-479-9876	Local	416-957-7340)
Markham office 905-479-9876	Toronto customer 416-957-7340	Local	905-479-9876
Toronto customer 416-957-7340	Uxbridge home 905-555-3467	Long distance	1-416-957-7340)
Uxbridge home 905-555-3467	Toronto customer 416-957-7340	Long distance	1-905-555-3467
Markham office 905-479-9876	Uxbridge home 905-555-3467	Long distance	1-905-479-9876
Uxbridge home 905-555-3467	Markham office 905-479-9876	Long distance	1-905-555-3467

Example: Defining dialing translations on the CallPilot servers

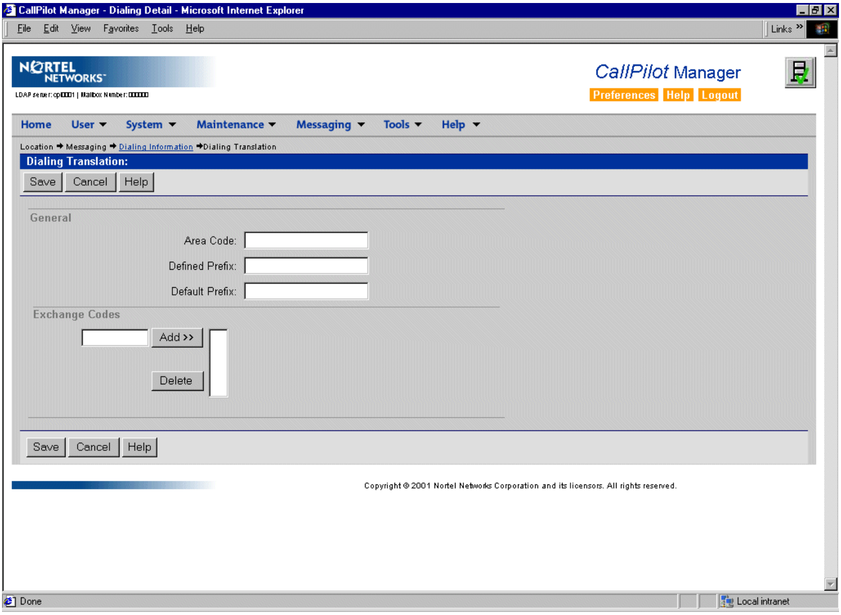
At Andrei’s office in Markham, as well as at the customer’s office in Toronto, the following is true for area code 905:

- There are only 5 exchanges for which all DNs are long distance calls: 555, 567, 579, 580, and 597.
- There are 50 exchanges for which all DNs are local calls.

If the Defined Prefix is used to indicate Long Distance calls, the administrator has to add only 5 exchange codes instead of 50. All calls to an area code combination of 905 and any other exchange are treated as local calls, as shown in the following table.

Setting	**Value**
Area Code	905
Defined Prefix	Long distance
Default Prefix	Local
Exchange Code list	555, 567, 579, 580, 597

Getting there Messaging → Dialing Information → Dialing Translations settings


CallPilot Manager - Dialing Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location ➜ Messaging ➜ Dialing Information ➜Dialing Translation
Dialing Translation:
Save Cancel Help
General
Area Code:
Defined Prefix:
Default Prefix:
Exchange Codes
Add >>
Delete
Save Cancel Help
Copyright © 2001 Nortel Networks Corporation and its licensors. All rights reserved.
Done
Local intranet

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring the dialing translations to handle mixed area or city codes by looking up **mixed area or city codes** in the CallPilot Manager online Help Index.

Defining address prefixes for both DTT and DTF

Introduction

Before you define address prefixes or dialing codes for delivery to telephone (DTT) or delivery to fax (DTF), check the guidelines.

Guidelines

When you configure DTT or DTF, consider the following requirements and recommendations:

- DTT and DTF addressing conventions
- DTMF confirmation
- automatically repeating the message

DTT and DTF addressing conventions

When you configure DTT or DTF addressing conventions, consider the following requirements and recommendations:

- dialing prefixes and codes
- synchronizing the DTT prefix and the dialing code
- prefixes for internal numbers
- a DTT prefix for each dialing scenario

Dialing prefixes and codes

To ensure that the DTT/DTF service is activated, you must define one or more dialing prefixes. Publish these prefixes so users can specify them during message composition and when entering addresses in distribution lists.

Cautions

- For each DTT prefix, you must also define an associated dialing code. When a user enters a DTT prefix, the system actually replaces the prefix the user entered with the associated dialing code. The dialing code is the public network access code that the system needs to place the call.
- DTT prefixes cannot conflict with mailbox numbers. If you have a coordinated dialing plan (CDP), the prefix can be the same as the initial number(s) of a CDP steering code, but cannot be the same as the entire code. For example, if one of your steering codes is 566, 5 or 56 can be used as a DTT prefix, but 566 cannot be used. For these cases, you need an arbitrary prefix that does not conflict with other numbers for the system to remove and replace with a dialing code to create a dialable number.

Synchronizing the DTT prefix and the dialing code

Make the DTT prefix and dialing code the same wherever possible. This simplifies message addressing for users because the numbers users enter when addressing a DTT message are exactly the same as the numbers they dial when placing an external call.

Example of synchronizing the DTT prefix and the dialing code

If the public network access code is 9, define both the DTT prefix and the dialing code as 9.

When a local caller enters 9-555-1212 as the DTF number, the access code 9 is replaced by the DTT prefix 9.

Prefixes for internal numbers

If you want to allow users to send DTT messages to internal extensions, you must set up a separate DTT prefix. This prefix is different, however, from others because it does not require an associated dialing code. Dialing codes are for access to the public network, and internal extensions are on your private network. When sending DTT messages to internal extensions, the prefix is simply stripped out of the address and the local extension is dialed. The prefix is needed to inform CallPilot to use the DTT service.

A DTT prefix for each dialing scenario

You need a DTT prefix and associated dialing code for each dialing scenario that you want to allow. This is because the system requires a different dialing code to place a call in each of the scenarios. For example, one dialing code (such as 9) is used to place local calls, whereas another (91) is used for long distance calls.

Dialing scenario	Example prefix	Corresponding dialing code
Internal: For internal extensions	56*	*none*
ESN: For numbers on your private ESN network, if you have one	6	6
Local: For local numbers on the public network	9	9
Long distance: For long distance numbers in the same country code	91	91
International: For long distance numbers with different country codes	9011	9011

DTMF confirmation

You can specify whether DTMF confirmation is required either on a user-by-user basis or on a system-wide basis.

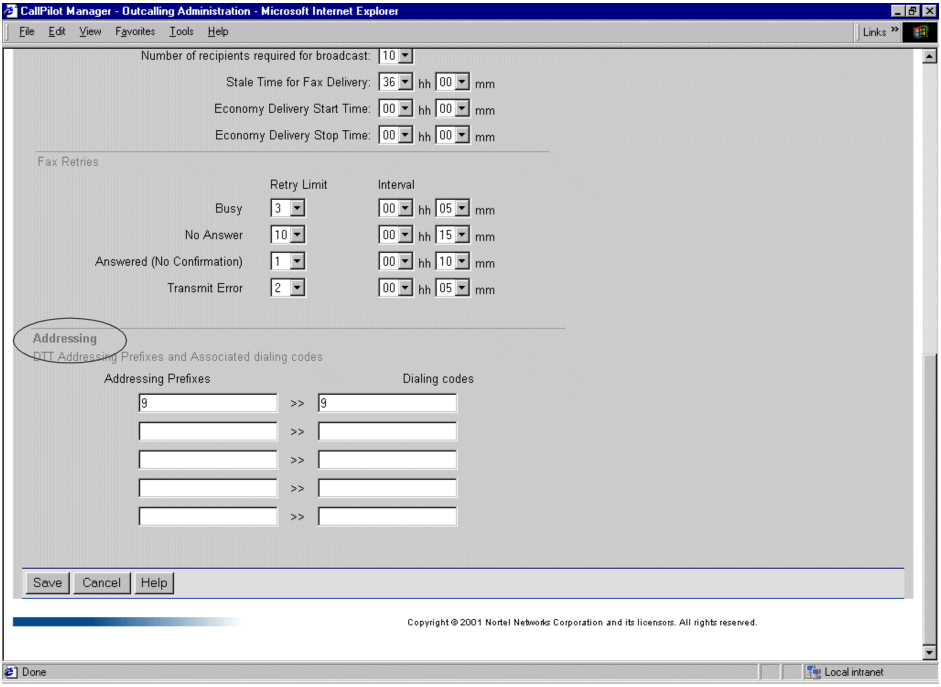
- If most users who receive DTT messages have rotary phonesets, disable DTMF confirmation for the entire system.
- If most users who receive DTT messages have answering machines, disable DTMF confirmation for the entire system.
- If users must be able to send messages to a diversity of recipients, such as in different parts of the world where there might or might not be DTMF support, enable or disable DTMF confirmation at the user level.

Automatically repeating the message

Some answering machine greetings contain a long pause, which might trigger the playback of the message before the greeting has finished. This means that the start of the DTT message will not be recorded since the greeting is still playing. Repeating the message makes it more likely that the entire message will be successfully recorded.

People who do not have a lot of experience with automated delivery of machine-generated messages might not realize what is happening initially. Playing the message twice increases the chance that they will be able to listen to the content of the message.

Getting there Messaging → Outcalling Administration → Addressing settings


CallPilot Manager - Outcalling Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links »
Save
Cancel
Help
Done
Local intranet

Number of recipients required for broadcast:	10			
Stale Time for Fax Delivery:	36	hh	00	mm
Economy Delivery Start Time:	00	hh	00	mm
Economy Delivery Stop Time:	00	hh	00	mm

Fax Retries

	Retry Limit	Interval			
Busy	3	00	hh	05	mm
No Answer	10	00	hh	15	mm
Answered (No Confirmation)	1	00	hh	10	mm
Transmit Error	2	00	hh	05	mm

Addressing

DTT Addressing Prefixes and Associated dialing codes

Addressing Prefixes		Dialing codes
9	>>	9
	>>	
	>>	
	>>	
	>>	

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

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring the DTT and DTF addressing conventions by looking up **addressing conventions** in the CallPilot Manager online Help Index.

Chapter 20

Configuring messaging service defaults

In this chapter

Enabling off-switch calls

Introduction

To enable mailbox owners to send messages to DNs that are off the local switch, you must:

- Specify the dialing prefixes that allow mailbox owners to call and send messages off the local switch.

  Note: This defines the dialing defaults that enable CallPilot features and custom applications to generate DNs for callbacks outside the local switch. These dialing defaults include the local prefix, the long distance prefix, the international prefix, and the ESN prefix.

- Specify the public network dialing codes of your local switch so that CallPilot can distinguish between private and public network calls.

  Note: These dialing codes include the local area code and the local country code.

ATTENTION

If your location must use multiple area codes for local calls, you must also define the dialing translations that enable CallPilot to distinguish between local and long distance calls for each mixed area code.

- Define how CallPilot is to treat a DN whose dialing format is not known.

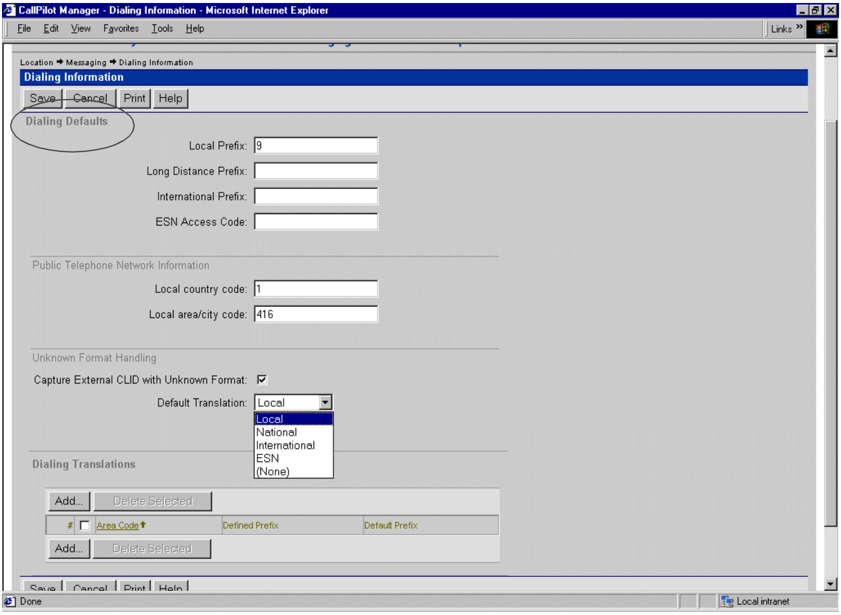
  Note: Typically, when an external caller calls a user at the local system and leaves a message for the local user, the switch passes to CallPilot both the caller’s number the type of this number (local, national, international, or ESN).

Connectivity restrictions

Only the Meridian 1 switch and the Succession CSE 1000 switch can capture an external CLID with an unknown format and then translate unknown dialing numbers into a default DN.

For all other switch types, the controls relating to CLID and the translation table are preset and disabled.

Getting there Messaging → Dialing Information → Dialing Defaults settings


CallPilot Manager - Dialing Information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Location → Messaging → Dialing Information
Dialing Information
Save Cancel Print Help
Dialing Defaults

Local Prefix: 9
Long Distance Prefix:
International Prefix:
ESN Access Code:

Local country code: 1
Local area/city code: 416

Capture External CLID with Unknown Format: ☑
Default Translation: Local

Looking up procedures in CallPilot Manager online Help

Find procedures for enabling off-switch calls by looking up **external calls** in the CallPilot Manager online Help Index.

Changing messaging defaults

Introduction

When you initially configure a CallPilot system, you can use the preconfigured messaging defaults. As you administer the system, you might need to change these defaults to accommodate

- a very large number of mailbox owners
- increased use of system resources
- changes in default billing or revert DNs, or introduction of a name dialing service
- the need to set up a special-purpose mailbox to store
  - faxes addressed to mailboxes that are not fax capable
  - *if messaging systems are networked:* messages relating to network diagnostics
  - messages generated by system alarms

Changing default messaging limits and warnings

To prevent messaging data and traffic from exceeding system capacity, configure mailbox limits for all mailbox owners.

Use the Messaging Management page to configure the following limits:

- maximum delay for timed delivery
- storage limits and warnings
- system time-outs

Maximum delay for timed delivery

Set the maximum number of days that message delivery can be delayed.

Default: 31 days

Valid range: 0 – 365

Storage limits and warnings

Setting	Description
Mailbox full warning threshold	The percentage of total messages that a mailbox can contain before the mailbox owner is given the mailbox full warning prompt at logon. **Default:** 85%
Maximum prompt size	Mailbox storage limits apply to all CallPilot voice items. When you specify the number of minutes and seconds allowed for user mailboxes, also specify the percentage at which CallPilot generates a warning to the user to delete voice items. **Default:** One minute, 30 seconds **Valid range:** 30 seconds – 9 minutes, 59 seconds
Maximum pages per fax item	Maximum number of pages for any single fax item. **Default:** 50 **Valid range:** 1 – 99
Minimum length of a Call Answering Message	The number of milliseconds that must be recorded in order for a call answering message to be saved as such. **Default:** 500 **Valid range:** 0 – 10000

System time-outs

Setting	Description
Command Entry	The Command Entry time-out is used when the system is waiting for a response from the caller. Set time parameters that, when exceeded, prompt the system for a response. **Example:** To prompt a caller after 2 seconds of non-response, enter 2000. **Default:** 3500 milliseconds **Valid range:** 1000 – 5000
Short Disconnect	The Short Disconnect time-out ends a call when the Command Entry time-out has been exceeded. Callers usually have several opportunities to respond before the short disconnect time-out is used. This time-out value is used when a caller disconnects from a thru-dial service or voice menu. **Example:** To configure CallPilot to disconnect a caller after two seconds of non-response, type 2000. **Default:** 10000 milliseconds **Valid range:** 1000 – 30000
Record	This time-out value is used when prompts are recorded for menus, announcements, and thru-dial services. The system disconnects the session when, during recording, the specified length of silence is recorded. **Example:** If the session is to be disconnected after one minute of silence, enter 60. **Default:** 120 seconds **Valid range:** 6 – 300

Changing the mailbox number length

CallPilot is shipped with a default mailbox number length of four digits.

To make it easier for users to remember their mailbox number, set the mailbox number the same as the extension. For example, if your organization uses five-digit extensions, change the mailbox number length to five digits.

Configuring default special-purpose DNs and prefixes

Configure the following special-purpose DNs.

Special-purpose DN	Description
Billing DN	The DN to accept billing charges if the caller’s mailbox number is somehow lost (if, for example, the call is dropped). **Number of digits:** 1 – 30
Revert DN	The DN to which callers are forwarded when they press 0 during a messaging or call answering session. **Number of digits:** 1 – 30

Special-purpose DN	Description
Optional: Prefix for Name Dialing and Name Addressing	The prefix that must be entered in order to dial a mailbox owner by name. **Example:** If Joe wants to compose a message to Jane, but doesn't know her mailbox or extension number, he can log on to his mailbox and 1 Dial 75 to compose the message. 2 Use the keypad to key the name dialing prefix (for example 11). 3 Key her last name and then her first name. **Number of digits:** Two **Default value:** 11

Name dialing and name addressing prefix

The name dialing prefix overrides any dialing options that are configured in the Thru-Dial block of custom applications and services. To prevent the override, use the Messaging Management page to disable the name dialing and name addressing feature.

Note: You can also disable the name dialing and name addressing feature to prevent external callers from identifying your system's users.

ATTENTION

Disable name dialing and name addressing features in countries where the keypads are not mapped to an alphabetical sequence that CallPilot recognizes.

See also

CallPilot Application Builder Guide

Specifying system-wide holiday service times

When you configure CallPilot messaging for your organization, specify the days and times of day when holiday service takes effect. This is referred to as the holiday service schedule.

The holiday schedule affects custom applications only. You can use Application Builder to configure an application to check every day of the week against the defined holiday service schedule.

ATTENTION

This holiday schedule has no effect on delivery times specified on the CallPilot Manager Message Delivery Configuration page.

Whenever you add a custom application in which the Day Control block checks for holidays, confirm the holiday service schedule definition.

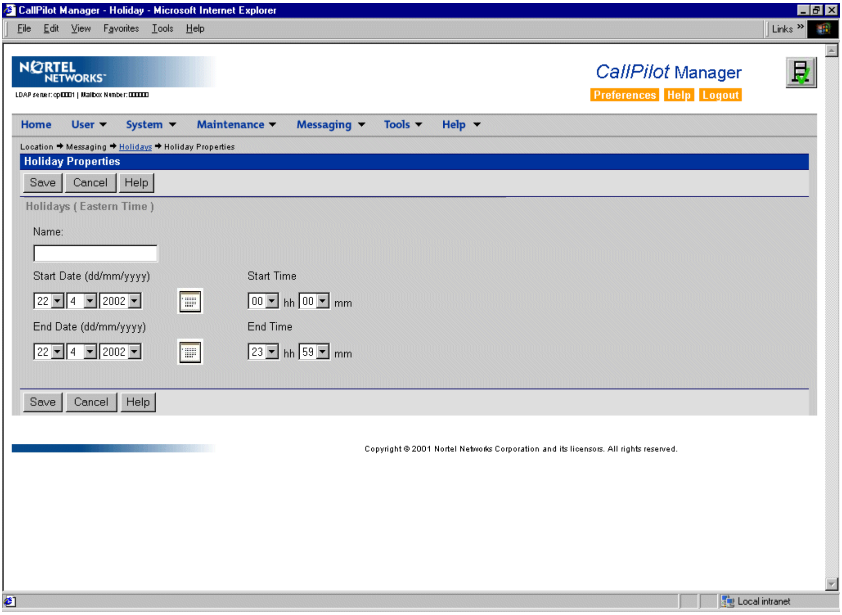
- If the holiday is not listed, add it.
- If the holiday does exist, ensure that it is properly defined. If not, change the holiday.
- Whenever a holiday becomes obsolete, delete it.

Information you need

To add or change a holiday, you must know

- the start and end dates of the holiday
- whether to define the holiday for a 24-hour day or for the business day

Getting there Messaging → Holidays → Holiday Properties



CallPilot Manager - Holiday - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help

Location ➔ Messaging ➔ Holidays ➔ Holiday Properties

Holiday Properties

Holidays (Eastern Time)

Name:

Start Date (dd/mm/yyyy) 22 4 2002

Start Time 00 hh 00 mm

End Date (dd/mm/yyyy) 22 4 2002

End Time 23 hh 59 mm

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

Looking up procedures in CallPilot Manager online Help

Find procedures for changing messaging defaults by looking up **messaging defaults** in the CallPilot Manager online Help Index.

Configuring special purpose mailboxes

Configuring the default fax general delivery mailbox

A general fax delivery mailbox provides one way for mailbox owners with voice-only mailboxes to receive fax messages.

ATTENTION

This fax general delivery mailbox does not handle fax overflows. For a procedure that provides fax general delivery for specific groups that provides for handling fax overflows, see Setting up mailboxes to handle fax deliveries and fax machine overflows.

Depositing messages

If a caller dials the express fax messaging SDN and enters a mailbox with no fax capability, a voice message informs the caller that the mailbox cannot receive faxes and offers the fax general mailbox as a destination. The caller can either accept the transfer of the fax message or hang up.

To deposit a message directly into the fax general delivery mailbox, a caller must dial the express fax messaging SDN from a faxphone.

Accessing messages

Anyone who knows the fax general delivery mailbox password can access all fax messages sent to it. Typically, an administrative assistant checks the mailbox periodically and distributes messages to individual recipients.

Note: You can also configure the general fax delivery mailbox to automatically print messages.

Privacy considerations and recommendation

The fax general delivery mailbox is like a system-wide bulletin board because all faxes sent to it are available to a large group of users.

Use the general fax delivery mailbox only for messages that do not contain proprietary or other confidential information. Mailbox owners who are likely to receive confidential information must have fax capability.

Configuring the system AMIS networking loopback mailbox

For information on using the AMIS networking loopback mailbox, refer to any of the networking administration guides.

Note: For links to online copies of these guides, open the Help menu at the top of any CallPilot Manager web page and click CallPilot Administration Help.

Configuring the system alarm mailbox

Define an alarm mailbox if you want CallPilot to send a voice message to a specified mailbox whenever an alarm is generated. The message notifies you that an alarm has been received. The message is tagged as urgent. After receiving a notification message, look at the Alarm Monitor to get more details.

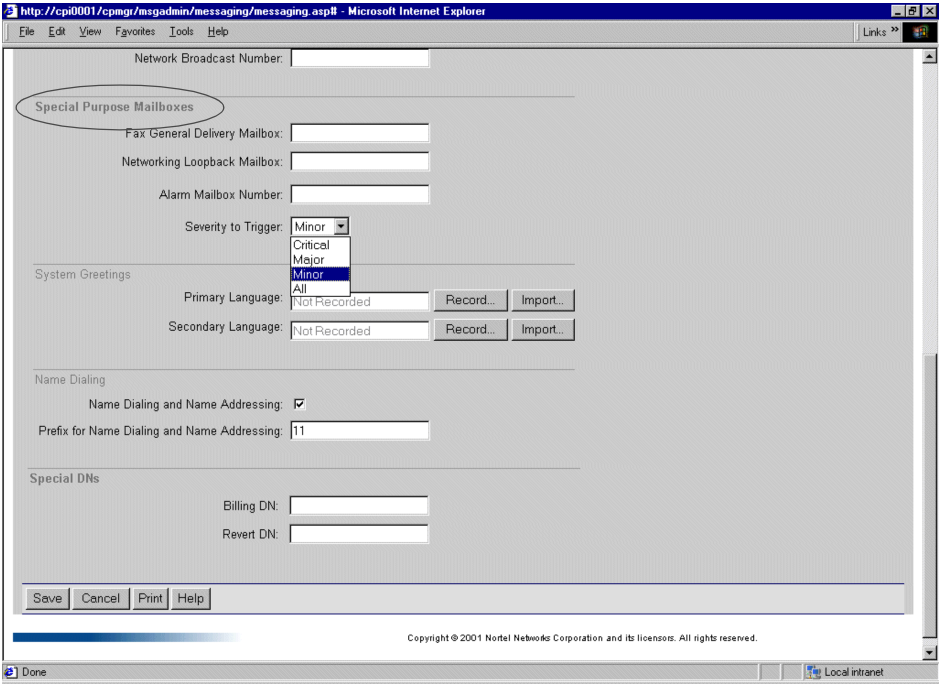
Nortel Networks recommends that this mailbox is configured for remote notification.

Immediate notification of alarm messages

If you want to be notified immediately of new alarms, enable remote notification for the alarm mailbox.

Note: Remote Notification must be enabled in the mailbox class which is applied to the alarm mailbox.

Getting there Messaging → Messaging Management → Special Purpose Mailboxes settings



http://cpi0001/cpmgr/msgadmin/messaging/messaging.asp# - Microsoft Internet Explorer

Network Broadcast Number:

Special Purpose Mailboxes

Fax General Delivery Mailbox:

Networking Loopback Mailbox:

Alarm Mailbox Number:

Severity to Trigger: Minor

System Greetings

Primary Language: Not Recorded

Secondary Language: Not Recorded

Name Dialing

Name Dialing and Name Addressing: ☑

Prefix for Name Dialing and Name Addressing: 11

Special DNs

Billing DN:

Revert DN:

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

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring special-purpose mailboxes by looking up **mailboxes** in the CallPilot Manager online Help Index.

Configuring mailboxes for fax deliveries and fax machine overflows

Introduction

To handle fax deliveries to owners of mailboxes with no fax capability, configure a fax general delivery mailbox. To handle the overflow from a busy or out-of-paper fax machine, set up a fax overflow mailbox.

Typically, owners of fax overflow mailboxes are administrators responsible for distributing incoming messages to the individuals they support. The mailbox owner distributes the messages stored in the fax general delivery mailbox.

- If a fax recipient has a mailbox with fax capability, the fax overflow mailbox owner can forward the message to the recipient’s mailbox.
- If a fax recipient does not have a fax-capable mailbox, the fax overflow mailbox owner can print the stored fax and distribute the printed copy to the recipient.

Note: Inform fax general delivery mailbox owners that the order that a mailbox receives faxes might not be reflected in the printing order.

Information you need

- fax general delivery mailbox number
- the fax machine DN (the number published as a group fax number)
- the default printing DN (if Autoprinting is enabled)

Task summary

1. On the switch, ensure the following are defined
   - a DN to be published as the fax number for a department or organization
   - a phantom DN to use as the fax general delivery mailbox number
2. Ensure the switch is provisioned so that
   - All Busy (Hunt) or No Answer calls to the fax machine are forwarded to the Multimedia Messaging SDN.
   - All calls to the Multimedia Messaging SDN are unconditionally forwarded to the fax machine DN.
   - All calls from the phantom DN are unconditionally forwarded to the fax machine.
   - All messages to the published fax mailbox are forwarded unconditionally to the fax machine designated for the group.
3. Using CallPilot Manager
   - Add the fax general delivery mailbox (a fax-capable mailbox with the phantom DN as the mailbox number).
   - Add the fax overflow mailbox (a mailbox, without fax capability, with the fax machine number as the mailbox number).
   - *Optional:* Configure remote notification of all fax general delivery mailbox owners.

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring fax deliveries and overflows by looking up **fax services** in the CallPilot Manager online Help Index.

Customizing system prompts

Introduction

CallPilot supplies a list of basic prompts for each language installed on the CallPilot server. If you install the CallPilot Player, you can listen to the supplied prompts and customize them to suit your CallPilot unified messaging system.

Once you have customized a system prompt, you can

- select either the supplied or the customized prompt
- edit the customized prompt as often as necessary

Note: To add new prompts, create a new custom application.

See also

CallPilot Application Builder Guide (555-7101-325)

Adding a corporate identity to system greetings

A system greeting is recorded by the administrator and precedes the personal greeting of all users during a call answering session.

You can customize the content of seven system prompts. You see these seven prompts in the main window of System Prompts Customization.

Example

“Welcome to RTM Productions, Online Products Division. Hello, this is Joanna Parker. I’m not at my phone right now. Please leave a message, and I’ll return your call as soon as possible.”

Note: The first sentence is the system greeting. The remainder of the message is the user’s personal greeting.

Viewing the lists of installed system prompts

CallPilot Manager displays a list of supplied system prompts for each installed language.

Listening to a system or custom prompt

Before you customize a prompt, listen to both the supplied system prompt and any customized prompt that has been used to replace the supplied prompt.

Limitation (Succession CSE 1000 switch)

When using your phoneset to listen to a system prompt, you must answer the phoneset within two or two-and-one-half ring cycles.

Before you can listen to a prompt, you must download the CallPilot Player.

See also

“Administrator shortcuts” topic in CallPilot Manager online Help.

Replacing a system prompt with a custom prompt

To replace a supplied system prompt with a custom prompt, you must be able to provide the customized prompt.

Note: Before you can provide a prompt, you must know the name and location of a suitable WAV file or have the CallPilot Player downloaded to your computer.

See also

“Administrator shortcuts” topic in CallPilot Manager online Help.

Editing a custom prompt

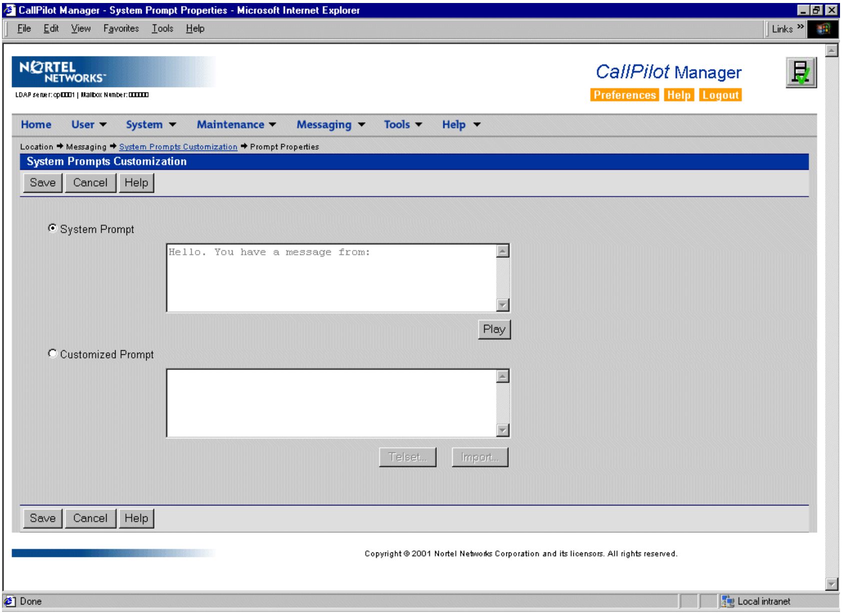
Before you can edit a prompt, you need either know the name and location of a suitable WAV file or have the CallPilot Player downloaded to your computer.

See also

“Administrator shortcuts” topic in CallPilot Manager online Help.

Getting there

Messaging → System Prompt Customization → Prompt Properties



CallPilot Manager - System Prompt Properties - Microsoft Internet Explorer

LDAP server: cp[redacted]1 | Mailbox Number: [redacted]

Location → Messaging → System Prompts Customization → Prompt Properties

System Prompts Customization

● System Prompt

Hello. You have a message from:

○ Customized Prompt

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

Looking up procedures in CallPilot Manager online Help

Find procedures for customizing system prompts by looking up **system prompts** in the CallPilot Manager online Help Index.

Configuring delivery to DNs not associated with CallPilot mailboxes

Introduction

An outbound SDN is required for message delivery to DNs that are not associated with mailboxes. Typically, this outbound SDN is one of the default SDNs on the switch and is automatically included in the SDN Table. You cannot create an outbound SDN in the SDN Table.

Outbound SDNs used for message delivery to non-mailbox DNs are Delivery to Telephone (DTT) and Delivery to Fax (DTF). In CallPilot Manager, these services are referred to as *outcalling services*.

Enable outcalling services for mailbox class members that must be able to compose and send voice or fax messages to phonesets, whether or not they have mailboxes associated with them.

Delivery to fax (DTF) versus fax messaging

Fax messaging service and DTF service differ in the following ways:

- Fax Messaging allows transmission of fax messages between CallPilot mailbox users.
- DTF service allows users to send faxes to external faxphones.

Delivery of messages with both voice and fax components

For messages that contain both voice and fax, CallPilot assumes that the address is either a telephone number or a fax number. Based on how the call is answered, the system sends the voice part, the fax part, or both parts of the message.

The DTT service is used to send the voice portion of a multimedia message addressed to an external recipient. DTT has its own defined time periods during which CallPilot is permitted to send DTT messages. In this case, messages are checked against the intersection of the DTT and DTF time ranges.

Example

Assume that

- The allowed DTT delivery time is 9:00 a.m. to 8:00 p.m.
- The allowed DTF delivery time is 8:00 a.m. to 11:00 p.m.

The allowed delivery time for a message containing both voice and fax components is 9:00 a.m. to 8:00 p.m. (the period of time that overlaps the two allowed delivery time periods).

Multi-delivery to fax service

Configuration of the multi-delivery to fax SDN determines the number of channels that can be allocated to large-scale external fax distributions. You can configure this service to specify the number of recipients to which an external fax message must be addressed before it will be handled by the multi-delivery to fax service instead of the delivery to fax (DTF) SDN.

The advantages of making this distinction are

- Each SDN can be allocated to different channels to help manage resources.
- You can temporarily reconfigure your system to increase the CallPilot resources dedicated to performing a large-scale fax distribution. By default, no channels are guaranteed for this service.

See also

- “Example 2: Allocations for large-scale external distributions of fax messages” on page 425
- CallPilot Manager online Help topic “Configuring multi-delivery to fax service.”

Task summary for setting up outcalling services

1 *For delivery to telephone (DTT):* Specify the DTT playback options.

Playback can be activated when the recipient provides DTMF input to confirm playback, or it can be voice-activated. DTT messages can be set to play either once or twice.

1 *For delivery to fax (DTF):* Define the number of recipients required for the delivery to be considered large-scale.

Large-scale external fax distributions use the multi-delivery to fax SDN instead of the DTF SDN. Each SDN can be allocated to different channels to help manage resources.

2 Define the number of recipients required for a fax delivery to use the multi-delivery to fax SDN instead of the DTF SDN.

Each SDN can be allocated to different channels to help manage resources.

3 Specify delivery times for DTT, DTF, and mixed media messages.

Attention: Local laws might not permit delivery of machine-generated messages at certain times of the day. You are responsible for determining these times and ensuring that the allowed delivery time does not overlap with restricted hours.

4 Define a retry strategy for DTT or DTF.

The conditions that can lead to a delivery failure are listed in the Delivery to telephone section of the Outcalling Administration page. Define for each condition how often and how many times the system will try to re-send a message if a delivery attempt is unsuccessful.

5 Define address prefixes for both DTT and DTF

Define the prefixes that users must enter when addressing messages to non-mailbox numbers. Define one prefix for each type of call you want to support (such as local and long distance). For each prefix, specify the dialing code (public network access code) that the switch requires to place the call. In most cases, make the prefix and the dialing code identical.

6 Test the DTT or DTF configuration.

7 Assign RPLs to features.

8 Specify the user’s RN information.

See also

For information about defining stale times, see the CallPilot Manager online Help topic “Specifying the DTT or DTF message delivery options.”

Reports on deliveries to external DNs

You can view the average and maximum times that each service had to wait to acquire a channel.

Run the following reports to determine if services that deliver messages to external DNs are able to acquire channels when needed:

- DTT Activity report
- Fax Deliveries Activity report
- Fax on Demand Audit Trail Detail report
- Fax Print Audit Trail Detail report
- RN Activity report
- RN Audit Trail Detail report

See also

CallPilot Manager online Help topic “Running reports”

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring DTT and DTF services by looking up **outcalling services** in the CallPilot Manager online Help Index.

Find the procedure for configuring the multi-delivery to fax SDN by looking up **fax services** in the CallPilot Manager online Help Index.

Find procedures for collecting report data and running reports by looking up **reports** in the CallPilot Manager online Help index.

Chapter 21

Configuring CallPilot services

In this chapter

Overview

Introduction

To make a service or application available to callers, you must add a unique service directory number (SDN) to the SDN Table and then publish the number to users of the service. Until you do this, the service or application exists in the system but callers cannot use it.

Note: Services that require an outbound SDN before they can perform their functions are automatically added to the SDN Table during software installation.

SDNs and service behavior

In addition to providing a unique dialable number for each CallPilot service, the SDN configuration also determines certain aspects of the service's behavior.

SDNs correspond to numbers that have been configured on the switch. Each SDN you enter in the SDN Table must correspond to one of the following numbers on the switch:

- the controlled DN of an ACD queue
- the DN of a phantom TN

Multiple SDNs for a single service

Create more than one service directory number (SDN) for a service when you must configure different session profiles for different user groups.

Example 1

Whenever a block in an application must behave differently from other blocks in the application, create the block as a separate application instead of as a block within a single application. Then you can configure the session profile for each use of the application block. For more information, refer to the *CallPilot Application Builder Guide* (555-7101-325)

Example 2

If your CallPilot system supports multiple languages for Fax Item Maintenance, Voice Item Maintenance, Speech Activated Messaging, or Paced Speech Messaging, create an SDN for each supported language, for each service.

Inbound SDNs

Inbound SDNs are required for dialable services. The SDN is the number that callers dial to access the service. You must add these SDNs to the CallPilot Manager SDN Table. After you add an SDN you can change its default configuration.

Outbound SDNs

Outbound SDNs are added to the SDN Table automatically during installation. Outbound SDNs are not dialed by callers. They are used by the system to place outbound calls and to determine the channel resources allocated to the service. You cannot use CallPilot Manager to create or modify outbound SDNs.

Typically, default outbound SDNs listed in the SDN table include:

- OUTBOUND11 (Remote Notification)
- OUTBOUND15 (Multi-delivery to Fax)
- OUTBOUND18 (Desktop Telephony Agent)
- OUTBOUND6 (Admin Agent)
- OUTBOUND7 (Delivery to Telephone)
- OUTBOUND8 (Delivery to Fax)

If the Networking feature is provided, all networking solutions are installed automatically. These include

- OUTBOUND9 (Enterprise Networking)
- AMIS Networking

If your system was purchased with the appropriate keycode, there might also be a Multimedia Messaging SDN.

Restrictions on editing outbound SDNs

Outbound Service Directory Numbers (SDNs) are automatically created by the system during installation. You cannot change the following:

- You cannot create or delete an outbound SDN.
- You cannot rename an outbound SDN.
- You cannot change the actual SDN.

  This number is specific to each service and is automatically assigned.
- You cannot modify the session profile or callback handling properties.

Adding inbound SDNs

Introduction

To make a custom application available to mailbox owners or callers, add the SDN to the CallPilot SDN Table.

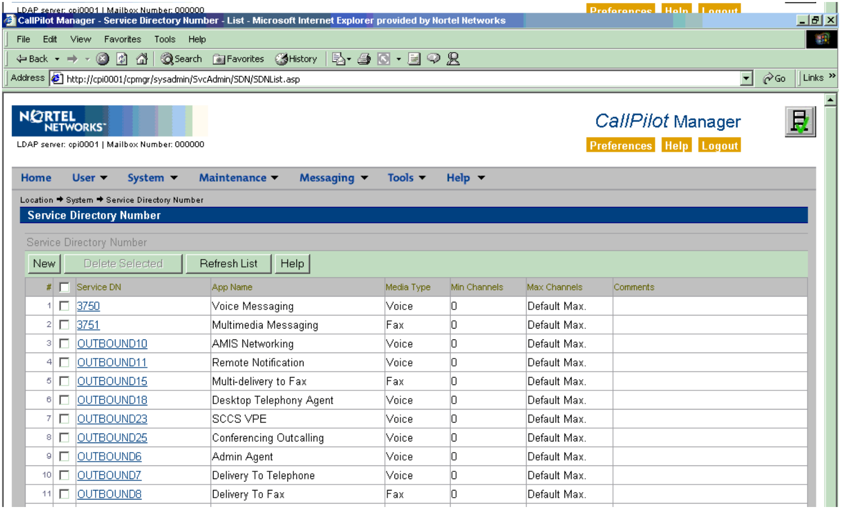
When a custom application becomes obsolete, delete the SDN.

Note: You cannot add or delete an outbound SDN.

Information you need

You must know the controlled DN or phantom TN configured on the switch for the service you are adding.

Getting there System > Service Directory Number


CallPilot Manager - Service Directory Number - List - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/sysadmin/SvcAdmin/SDN/SDNList.asp
Go Links
NORTEL NETWORKS
LDAP server: cpi0001 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location System Service Directory Number
Service Directory Number
Service Directory Number
New Delete Selected Refresh List Help

#	□	Service DN	App Name	Media Type	Min Channels	Max Channels	Comments
1	□	3750	Voice Messaging	Voice	0	Default Max.	
2	□	3751	Multimedia Messaging	Fax	0	Default Max.	
3	□	OUTBOUND10	AMIS Networking	Voice	0	Default Max.	
4	□	OUTBOUND11	Remote Notification	Voice	0	Default Max.	
5	□	OUTBOUND15	Multi-delivery to Fax	Fax	0	Default Max.	
6	□	OUTBOUND18	Desktop Telephony Agent	Voice	0	Default Max.	
7	□	OUTBOUND23	SCCS VPE	Voice	0	Default Max.	
8	□	OUTBOUND25	Conferencing Outcalling	Voice	0	Default Max.	
9	□	OUTBOUND6	Admin Agent	Voice	0	Default Max.	
10	□	OUTBOUND7	Delivery To Telephone	Voice	0	Default Max.	
11	□	OUTBOUND8	Delivery To Fax	Fax	0	Default Max.	

Looking up procedures in CallPilot Manager online Help

Find procedures for adding SDNs by looking up **SDNs** in the CallPilot Manager online Help Index.

Section A: Configuring messaging services

In this section

Configuring a session profile for messaging services or Application Builder services

Introduction

You must configure a session profile for

- any custom application voice menu or feature
- express voice messaging
- express fax messaging

When you configure a session profile, you can

- Limit the session length and number of consecutive invalid password entries to prevent malicious callers from using up your system’s resources.
- Specify an express voice messaging or express fax messaging mailbox number.
- Specify a language for the session if there is more than one language installed on the system.

Defining the broadcast message numbers

Introduction

Use the Messaging Management page to define the numbers that mailbox owners must specify when they compose broadcast messages.

Broadcast capabilities

Depending on the mailbox class, mailbox owners have one of the following levels of broadcast capability:

- no broadcast capability
- local broadcast capability (includes local location broadcast capability)
- both local broadcast and network broadcast (includes network location broadcast) capability

Local broadcast

A local broadcast is a voice message that is delivered to all of the users on the local system.

Location broadcast

A location broadcast is a message that is sent to all users at a specific remote site or switch location in the messaging network.

Network broadcast

A network broadcast is a message that is sent to all mailboxes at both local and remote sites (including switch locations) in the messaging network.

Impact on system resources

Extensive use of broadcast messages adds to the messaging traffic over the CallPilot system.

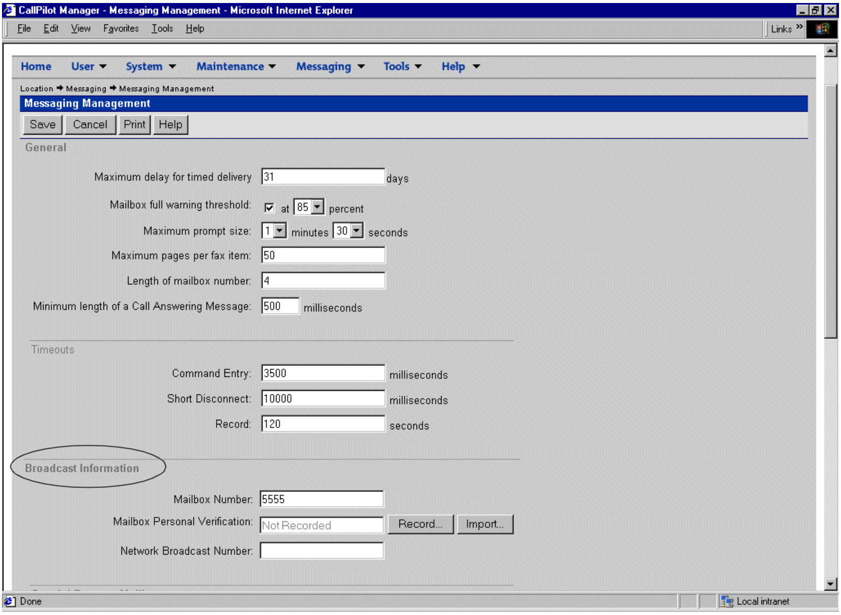
To minimize its use:

- Limit broadcast capability to the level that mailbox owners really need.
- Maintain a comprehensive list of shared distribution lists (SDLs) and enable SDL addressing for mailbox owners.
- Disable the exchange of broadcast messages between the local messaging server and one or more remote messaging servers

  Refer to “When to disable broadcast messages” in CallPilot Manager online Help.

Getting there

Messaging → Messaging Management → Broadcast Information settings


CallPilot Manager - Messaging Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Home
User
System
Maintenance
Messaging
Tools
Help
Location → Messaging → Messaging Management
Messaging Management
Save
Cancel
Print
Help
Record...
Import...
Done
Local intranet

General

Maximum delay for timed delivery: 31 days

Mailbox full warning threshold: ☑ at 85 percent

Maximum prompt size: 1 minutes 30 seconds

Maximum pages per fax item: 50

Length of mailbox number: 4

Minimum length of a Call Answering Message: 500 milliseconds

Timeouts

Command Entry: 3500 milliseconds

Short Disconnect: 10000 milliseconds

Record: 120 seconds

Broadcast Information

Mailbox Number: 5555

Mailbox Personal Verification: Not Recorded

Network Broadcast Number:

Looking up procedures in CallPilot Manager online Help

Find procedures for defining broadcast message numbers by looking up **broadcast messages** in the CallPilot Manager online Help Index.

Section B: Configuring Application Builder fax services

In this section

Configuring an Application Builder fax service

Introduction

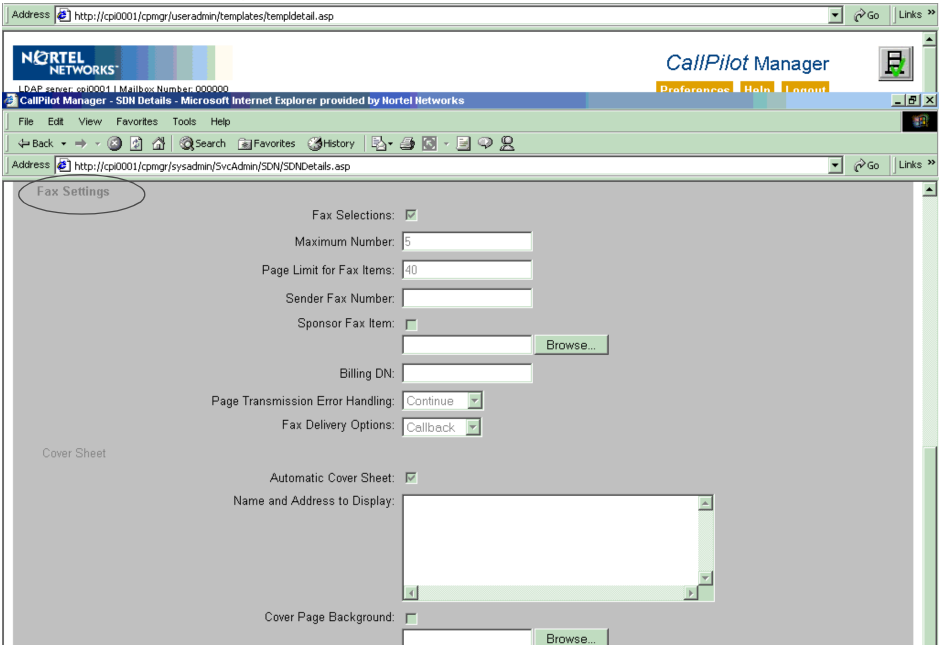
You must configure fax options for a fax feature (for example, express fax messaging) or custom application.

ATTENTION

If you do not specify a billing DN, chargeable calls are billed to the SDN.

Note: A custom cover page is recommended for each fax service.

Getting there System → Service Directory Number → Service Directory Number page → Fax Settings



Fax Settings

Fax Selections: ☑

Maximum Number: 5

Page Limit for Fax Items: 40

Sender Fax Number:

Sponsor Fax Item: □

Billing DN:

Page Transmission Error Handling: Continue

Fax Delivery Options: Callback

Cover Sheet

Automatic Cover Sheet: ☑

Name and Address to Display:

Cover Page Background: □

Address http://cpi0001/cpmgr/useradmin/templates/templdetail.asp
NORTEL NETWORKS
CallPilot Manager
LDAP server: cpi0001 | Mailbox Number: 000000
Preferences
Help
Logout
CallPilot Manager - SDN Details - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/sysadmin/SvcAdmin/SDN/SDNDetails.asp
Go Links
Browse...
Browse...

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring a fax service by looking up **fax services** in the CallPilot Manager online Help Index.

Configuring callback handling for a fax service

Introduction

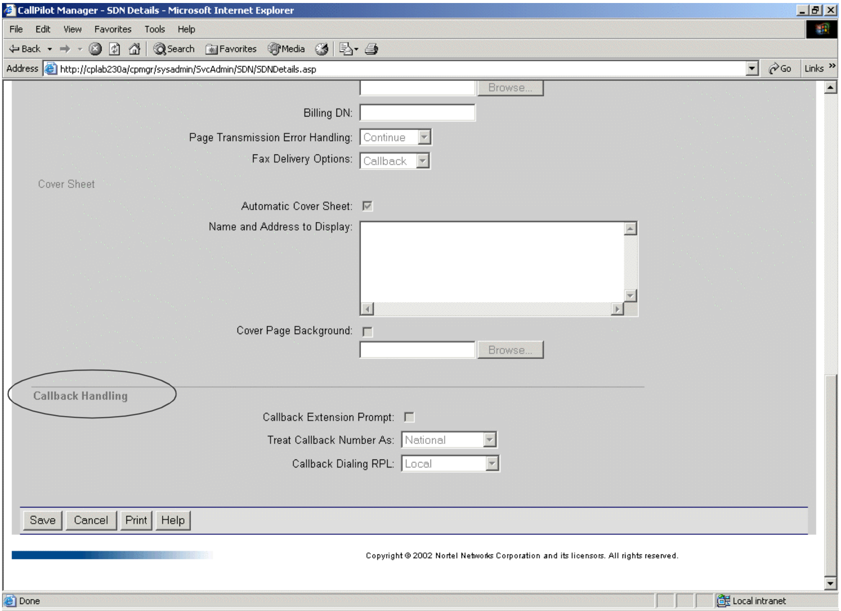
When planning callback handling options, identify how callback numbers must be treated for the service you are configuring. Callback numbers must be in a format that the system can use to generate a dialable number. This ensures that the requested fax items can be delivered.

CallPilot needs the correct access code to originate a telephone call from the switch. The treatment you select determines how callers are prompted to enter fax callback numbers.

- Ensure that callers are prompted to enter the necessary dialing codes, such as country code or area code.
- Identify the potential calling audience and where the members will be calling from.

Note: If all boxes are disabled, no further configuration is necessary.

Getting there System → Service Directory Number → Service Directory Number page → Callback Handling settings


CallPilot Manager - SDN Details - Microsoft Internet Explorer

Address http://cplab230a/cpmgr/sysadmin/SvcAdmin/SDN/SDNDetails.asp

Billing DN:

Page Transmission Error Handling: Continue

Fax Delivery Options: Callback

Cover Sheet

Automatic Cover Sheet: ☑

Name and Address to Display:

Cover Page Background: □

Callback Handling

Callback Extension Prompt: □

Treat Callback Number As: National

Callback Dialing RPL: Local

Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring a fax callback handling by looking up **fax services** in the CallPilot Manager online Help Index.

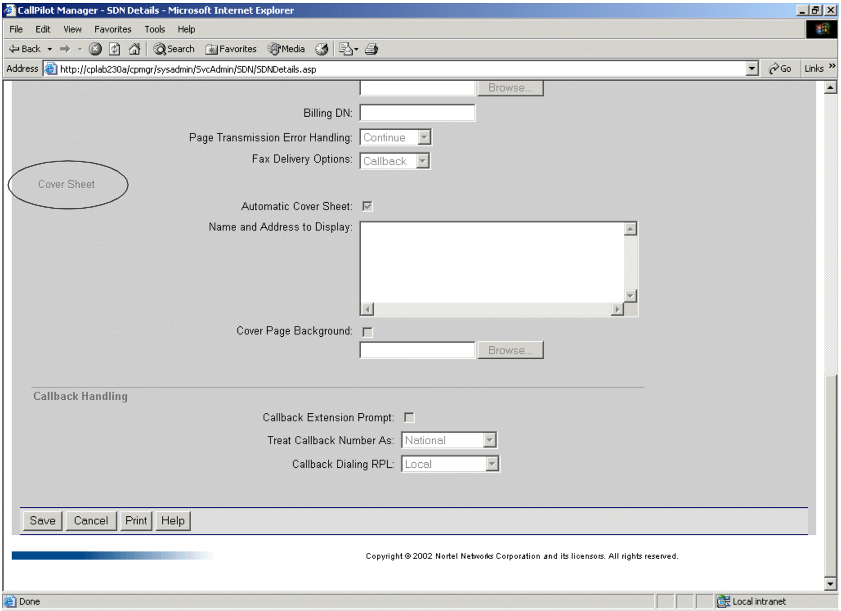
Configuring a custom cover page for a fax service

Introduction

A custom cover page is recommended for each fax service.

Getting there

System → Service Directory Number → Service Directory Number Details page → Fax Settings → Cover Sheet



CallPilot Manager - SDN Details - Microsoft Internet Explorer

Address: http://cplab230a/cpmgr/sysadmin/SvcAdmin/SDN/SDNDetails.asp

Billing DN:

Page Transmission Error Handling: Continue

Fax Delivery Options: Callback

Cover Sheet

Automatic Cover Sheet: ☑

Name and Address to Display:

Cover Page Background: □

Callback Handling

Callback Extension Prompt: □

Treat Callback Number As: National

Callback Dialing RPL: Local

Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring a custom fax cover page by looking up **fax services** in the CallPilot Manager online Help Index.

Section C: Configuring alternate phoneset interfaces

In this section

Overview

Introduction

Configure alternate phoneset interfaces to support new CallPilot mailbox owners who are accustomed to using another messaging system.

CallPilot supports use of two alternate phoneset interfaces:

- one similar to a widely-used command-based interface
- one similar to a widely used menu-based interface

Once all required configuration tasks are performed, mailbox owners can access a mailbox by using either the CallPilot Voice Messaging SDN, or the SDN configured for the alternate interface.

ATTENTION

As you add new mailbox owners that prefer an alternate phoneset interface, use an input data file that specifies the appropriate new mailbox class.

Educating mailbox owners

Refer mailbox owners to My CallPilot Useful Information for quick reference cards and command comparison cards for the alternate interfaces.

Automating the choice of phoneset interface for mailbox owners and callers

A Session Profile setting in the SDN definition controls whether or not the SDN interface style will override the mailbox owner’s preferred phoneset interface style. If this setting is disabled, callers to the standard Voice Messaging SDN are presented with the mailbox owner’s preferred phoneset interface style (following initial access to the mailbox).

Availability of CallPilot functions to users of alternate interfaces

Introduction

Because an alternative phoneset interface supports only core messaging functions, the mailbox owner must use the CallPilot interface or a web interface to access advanced multimedia messaging and mailbox administration functions.

Service access

CallPilot Messaging uses the called service directory number (SDN) to determine which application or service is to be offered. Individual services may then use the call record information to offer different options. For example, the logon service uses the call record information to determine whether to prompt for mailbox number or password.

Each alternative logon and call answering application incorporates a service menu.

The service menu lets the caller leave a message in a mailbox, dial an extension, or log on to a mailbox.

The user interface style for Call Answering is controlled by a mailbox class setting (Phoneset interface for mailbox callers).

Limitations

- Alternate phoneset interfaces do not provide the following prompts and commands:
    - the extended message header

      Alternate phoneset interfaces provide the short message header option only.
    - the “on the phone” notification prompt
    - the administrative prompts such as those for recording the system greeting or another mailbox owner's personal verification.
    - the commands to create or print fax messages
    - remote notification or remote text notification administration prompts and commands

      Mailbox owners with these capabilities must use the CallPilot UI to configure notification settings.
    - prompts or commands for maintenance of personal distribution lists (PDLs)

      Invalid PDL entries are not auto-deleted.
    - DTMF Confirmation Required for DTT prompt
    - the CallPilot economy delivery option
- Speech activated messaging provides only CallPilot prompts and commands. Users may find speech activated messaging to be unfamiliar in organization.
- Alternate phoneset interfaces provide prompts and commands for autoprinting fax messages and for printing a fax separator page, but not for administering those functions.
- Callers who access a mailbox via name dialing do not receive prompts provided by alternate phoneset interfaces.
- There are several prompt terminology differences among the phoneset interfaces. For example, “press number sign” instead of “press the pound key” may be confusing to alternate phoneset interface users.
- The revert DN works only if the caller presses zero before the end of the mailbox owner's recorded greeting.

Configuration tasks

Task summary

This configuration allows mailbox owners to be transitioned to the CallPilot phoneset interface without requiring new logon DNs.

1. Ensure that the mailbox class setting determines the phoneset interface for all mailbox callers. See “Ensuring use of the preferred phoneset interface” on page 411.
2. Create a CallPilot Voice Messaging SDN that ensures that the use of the selected alternate interface overrides the phoneset interface specified in the mailbox class. See “Making the alternate phoneset interface available to users” on page 413.
3. Create mailbox classes for the alternative interface users and configure them with the mailbox owner's preferred phoneset interface. To ensure you have all required mailbox classes, you can duplicate each existing mailbox class and then configure the call answering options to use the preferred phoneset interface. See “Creating and deleting mailbox classes” on page 342 and “Configuring mailbox classes” on page 343.
4. Apply the appropriate new mailbox class to each existing mailbox owner who prefers the alternate phoneset interface. See “Changing a mailbox owner's mailbox class” on page 302.

See also

For specific instructions, refer to the CallPilot Manager online Help book “Allowing use of an alternate phoneset interface.”

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring alternate phoneset interfaces by looking up **alternate phoneset interfaces** in the CallPilot Manager online Help Index.

Ensuring access to features exclusive to CallPilot

Introduction

Because an alternative user interface supports only core messaging functions, the mailbox owner must use the CallPilot voice messaging interface, desktop messaging, or My CallPilot to access advanced multimedia messaging and mailbox administration functions.

ATTENTION

To ensure that all mailbox owners can access CallPilot features not supported by alternate phoneset interfaces, configure a second Voice Messaging SDN with the SDN override enabled.

Storage management

The alternate phoneset interfaces use the automatic deletion strategy configured for CallPilot. Expiry periods for saved messages are configured in the mailbox class resource usage controls.

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring alternate phoneset interfaces by looking up **alternate phoneset interfaces** in the CallPilot Manager online Help Index.

Ensuring use of the preferred phoneset interface

Introduction

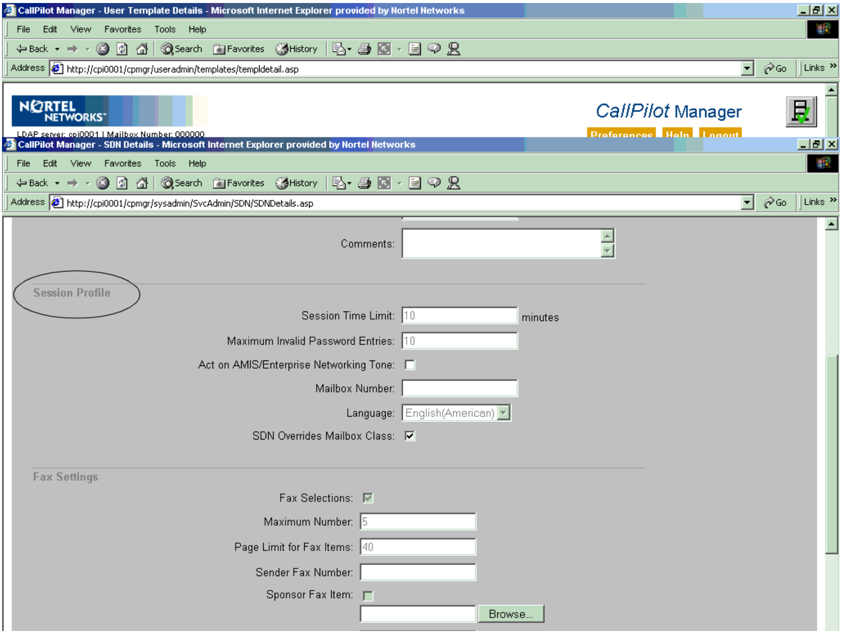
By default, the mailbox class determines the set of phoneset commands presented to the mailbox owner following logon to the mailbox.

If many CallPilot mailbox owners are accustomed to using another voice messaging system, you might want to configure an alternate phoneset interface and corresponding mailbox classes.

SDN override

Leave the SDN override disabled if you want to configure some mailboxes to present an alternate phoneset interface, or to allow mailbox owners to determine which phoneset interface will be presented.

Getting there System → Service Directory Number → Service Directory Number page → Session Profile



CallPilot Manager - User Template Details - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/useradmin/templates/templdetail.asp
Go Links
NORTEL NETWORKS
CallPilot Manager
LDAP server: cpi0001 | Mailbox Number: 000000
Preferences Help Logout
CallPilot Manager - SDN Details - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://cpi0001/cpmgr/sysadmin/SvcAdmin/SDN/SDNDetails.asp
Go Links
Browse...

Comments:

Session Profile

Session Time Limit: 10 minutes

Maximum Invalid Password Entries: 10

Act on AMIS/Enterprise Networking Tone: ☐

Mailbox Number:

Language: English(American)

SDN Overrides Mailbox Class: ☑

Fax Settings

Fax Selections: ☑

Maximum Number: 5

Page Limit for Fax Items: 40

Sender Fax Number:

Sponsor Fax Item: ☐

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring alternate phoneset interfaces by looking up **alternate phoneset interfaces** in the CallPilot Manager online Help Index.

Making the alternate phoneset interface available to users

Introduction

To make an alternate phoneset interface available to mailbox owners or callers, you must add a voice messaging SDN to the CallPilot SDN Table.

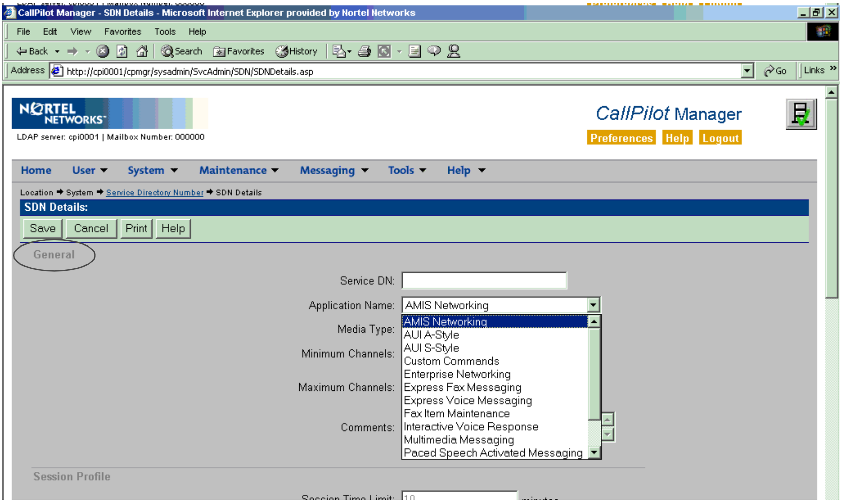
ATTENTION

To ensure the mailbox owner is presented with the alternate phoneset commands following logon to the mailbox, configure the SDN so that the phoneset interface associated with the SDN overrides the phoneset interface specified in the mailbox class.

Information you need

The controlled DN or phantom TN configured on the switch for this service

Getting there System → Service Directory Number → Service Directory Number Details page → General


CallPilot Manager - SDN Details - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Save Cancel Print Help
General
Session Profile

http://cpi0001/cpmgr/sysadmin/SvcAdmin/SDN/SDNDetails.asp

LDAP server: cpi0001 | Mailbox Number: 000000

Location → System → Service Directory Number → SDN Details

SDN Details:

Service DN:

Application Name: AMIS Networking

Media Type:

Minimum Channels:

Maximum Channels:

Comments:

AMIS Networking
AUI A-Style
AUI S-Style
Custom Commands
Enterprise Networking
Express Fax Messaging
Express Voice Messaging
Fax Item Maintenance
Interactive Voice Response
Multimedia Messaging
Paced Speech Activated Messaging

Session Time Limit: 10 minutes

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring alternate phoneset interfaces by looking up **alternate phoneset interfaces** in the CallPilot Manager online Help Index.

Section D: Configuring Symposium Voice Services support

In this section

Overview

Introduction

Symposium Voice Services support

- provides unified messaging to Symposium Call Center personnel
- allows use of a single server to provide both messaging and voice services
- allows customers who install multiple keycoded unified messaging components (for example: fax messaging, desktop messaging and My CallPilot, or E-mail By Phone) to purchase a CallPilot system with integrated Symposium Voice Services features
- is fully backward compatible with current Meridian Mail Voice Services support

A maximum of 96 CallPilot voice channels can be allocated for Symposium Voice Services support.

Voice Services call flow

1. The switch informs the Symposium Call Center server that a call has arrived at the IVR CDN.
2. The Symposium Call Center server routes the call to the ACCESS CDN.
3. The switch sends the call to a CallPilot ACCESS channel. The Meridian Link TSP alerts CallPilot and CallPilot informs the Symposium Call Center server of the call coming in over the ACCESS link.
4. The Symposium Call Center server controls playing of voice segments and collection of digits over the ACCESS link.

Feature architecture

- On the CallPilot server, channels are allocated to either messaging services or Symposium Voice Services.

- The Symposium Call Center server acquires voice port TNs from the switch via the AML and voice port channels from CallPilot vial the ACCESS link.
- Custom applications (created and maintained in Application Builder) are used to administer voice prompts. Voice prompts can be edited using third party applications.
- The CallPilot database stores the following information:
  - the Symposium Call Center server IP address on the customer LAN
  - the TNs of all ACCESS and IVR ports
  - the key 0 and key 1 DNs of all ACCESS and IVR channels
  - the channels that are reserved for ACCESS or IVR
- The CallPilot server registry stores the ACCESS link port number.
- Resources acquired by the Symposium Call Center server are associated with its Application Module Link (AML) connection.

ATTENTION

AML allows resources to be associated with one AML connection only. This means that CallPilot's AML connection with the switch cannot be used to control voice channels already acquired by Symposium.

- The switch communicates with CallPilot via the Symposium Call Center server and the Meridian Link Services Module (MLSM).
- ACCESS and IVR channels support voice media only and each channel uses one DSP. CallPilot ACCESS class IDs identify ACCESS channels. If you are migrating from Meridian Mail to CallPilot 2.02, note the following architecture changes:
- The TCP/IP (ELAN) ACCESS link between the CallPilot server and the Symposium Call Center server replaces the serial ACCESS link between Meridian Mail and the Symposium Call Center server.
- CallPilot does not support the communication link (CSL) used between Meridian Mail and the switch.

System requirements

- Symposium Call Center Services (SCCS) release 4.2 on a PVI platform with the NS040206CPSU07S performance enhancement
- CallPilot 2.0 or later
- Depending on the switch, either of the following:
  - Meridian 1 X11 software Release 24.24 or later
  - Succession CSE 1000 Release 1.1 or later

Voice port requirements

Voice port configuration must be consistent across the switch, the Symposium Call Center server, and the CallPilot server. This means that the following:

- Each voice port TN configured on the switch and the Symposium Call Center server are also be configured on the CallPilot server.
- The CDN configured on the switch for ACCESS channels is configured as the Symposium Voice Services CDN in the CallPilot SDN table.
- The CDN for IVR channels is configured as an Application Builder voice menu or announcement in the CallPilot SDN table.
- the Class ID matches those configured on the Symposium Call Center server and the switch.

See also

- Part 3 of the *CallPilot Installation and Configuration* binder for your server platform
- *CallPilot Application Builder Guide* (NTP 555-7101-325)
- *Meridian Mail to CallPilot Migration Utility Guide* (NTP 555-7101-801)
- *Symposium 4.2 Meridian 1/Symposium CSE 1000 Voice Processing Guide*

Configuration tasks

Task summary

1. On the switch:
   - Configure separate embedded LAN (ELAN) and value added server (VAS) IDs for Symposium Call Center and CallPilot.
   - In addition to the CDNs configured for CallPilot messaging agents, configure a CDN for the ACCESS agent and a CDN for the IVR agent.
   - Configure each ACCESS and IVR port.
2. On the CallPilot server:
   - Use the Configuration Wizard to enter the Symposium Call Center server IP address on the customer LAN, the terminal numbers for the IVR and ACCESS channels, and the IVR and ACCESS channel allocations.

     ATTENTION

     The channel number assigned to the ACCESS port on the Symposium Call Center server must match the Class ID that is configured in CallPilot's channel allocation.

   - Use CallPilot Manager to add service DNs for Symposium Voice Services (the ACCESS CDN) and the Application Builder announcement or voice menu (the IVR agent CDN).

See also

For Configuration Wizard procedures, refer to the CallPilot Manager online Help book “Reconfiguring the system.”

For the procedure to add the SDNs, refer to the CallPilot Manager online Help book “Configuring Symposium Voice Services support.”

For help with troubleshooting, see “Troubleshooting Symposium Voice Services support” on page 530.

Looking up procedures in CallPilot Manager online Help

Find procedures for configuring alternate phoneset interfaces by looking up **Symposium Voice Services support** in the CallPilot Manager online Help Index.

Section E: Allocating channels to services

In this section

Dynamic channel allocations

Introduction

By default, CallPilot allocates channels to services dynamically, based on available channel resources. For most systems, this default configuration works very efficiently.

ATTENTION

The total number of channels available for any CallPilot system is keycode-controlled. If you need more channels, upgrade your CallPilot server.

The default minimum

The minimum number of channels allocated to each service is zero. This means that services are not guaranteed access to any channels. Other services are allowed to use all of the channels of a particular type (such as fax), leaving no available channels.

How **the default minimum channel allocation for a service works**

- When a Fax on Demand service is configured with the default minimum channel allocation of zero (0), no channels are dedicated to this service.
- Whenever all fax channels on the system become busy due to traffic generated by other fax services, a call in to the Fax on Demand service is queued until a fax channel becomes idle.

The default maximum

By default, the maximum number of channels that a service can use at any one time is all channels of the required type.

How the default maximum channel allocation for a service works

- Four fax channels are on your system. A Fax on Demand service is configured with the default maximum channel allocation. This means that no fax channels are reserved for other fax services.

- Whenever a burst of traffic is directed at the Fax on Demand service, this service is allowed to use all available fax channels simultaneously, leaving no channels available to other fax services.

Allocations for applications with fax callback

If the session profile for an application allows fax callback delivery, the channel allocations assigned to the service’s SDN are not used. Instead, the channel allocations assigned to the Delivery to Fax SDN are used, because the Delivery to Fax service delivers faxes on a callback.

Allocations for speech recognition services

Speech recognition channels use four times the processing power of multimedia channels.

Monitoring service demand

Run the Reporter System Traffic Summary report to identify how much particular services are used. For example, you can identify the percentage of total traffic generated by a service. This gives you an idea of whether the current channel allocations for that service are adequate.

Estimating service requirements

Use the guidelines in the *CallPilot Planning and Engineering Guide* (555-7101-101) to estimate the number of channels a service needs. Then use Reporter to monitor actual service usage to see if you must adjust the channel allocations.

Re-allocating channels

Introduction

You can change the minimum number of channels guaranteed for a service. This is useful whenever traffic generated by the service is greater than originally anticipated or for temporary high demand on a service.

The way you allocate channels during times of normal operation depends on factors such as

- how much traffic you expect the service to generate
- the importance of the service.

ATTENTION

Nortel Networks strongly recommends that you do not re-allocate channels to services unless you experience problems making an essential service available to users. Verifying a new allocation scheme for all services can be time-consuming. See “Re-allocating channels” on page 424.

Examples

This section provides several examples of how channels might be re-allocated temporarily to accommodate atypical demand on a service.

Example 1: A new voice menu application is put into service

This menu informs company employees of the new benefits plan, and is expected to generate heavy traffic during the first month it is used.

Your system has 18 voice channels. For the first month of service, you allocate a minimum of two channels and a maximum of four channels to the voice menu.

After one month, when the amount of traffic generated by the service decreases, you reduce the minimum number of channels to zero and the maximum to two.

- A minimum setting of zero means that the service is not guaranteed any channels. If all voice channels are busy, the service cannot obtain a channel until there is an idle channel.
- A maximum setting of two means that the service cannot use more than two of the 18 voice channels simultaneously. Sixteen channels are reserved for use by other voice services.

Example 2: Allocations for large-scale external distributions of fax messages

You can temporarily reconfigure your system to increase the CallPilot resources dedicated to performing a large-scale fax distribution. By default, no channels are guaranteed for this service.

Requirements and recommendations

Before you can allocate additional resources to a large-scale external fax distribution, you must configure the threshold that determines the meaning of “large-scale.”

Nortel Networks strongly recommends that you use the altered channel allocation on a temporary basis only, and during off-peak hours.

ATTENTION

Mailbox owners who are responsible for large-scale external fax distributions must time delivery of the fax messages to coincide with the temporary channel re-allocation.

Configuring the threshold

The number of channels that can be simultaneously allocated to deliver fax broadcast messages is determined by the configuration of the multi-delivery to fax SDN. The delivery to fax (DTF) SDN handles external deliveries of fax messages that are addressed to a lower number of recipients than is configured for the multi-delivery to fax service.

See also

- “Multi-delivery to fax service” on page 384
- “Dynamic channel allocations” on page 422
- “Re-allocating channels” on page 424
- *For configuring the maximum delay for timed delivery:* “Changing messaging defaults” on page 368

Getting there

System → Service Directory Number → SDN Details

Looking up procedures in CallPilot Manager online Help

For procedures to re-allocate channel resources, refer to CallPilot Manager online Help. Open the “Configuring CallPilot services” book, and then open the “Allocating channels to services” book. You can also look up **channel allocations** in the Index.

Section F: Configuring and troubleshooting Email-by-Phone

In this section

Configuring Email-by-Phone

Configuring Email-by-Phone using CallPilot Manager

This section provides the procedures for configuring the Email-by-Phone feature using CallPilot Manager. Before starting these procedures, ensure that all the required CallPilot server performance enhancement packages (PEP) have been applied. The PEPs specific to the Email-by-Phone feature are as follows:

- CP20126G053S
- CP20126G059S

Note: These PEPs require that the CallPilot server be installed with, or updated to, service update 1 (SU-01).

Procedure summary

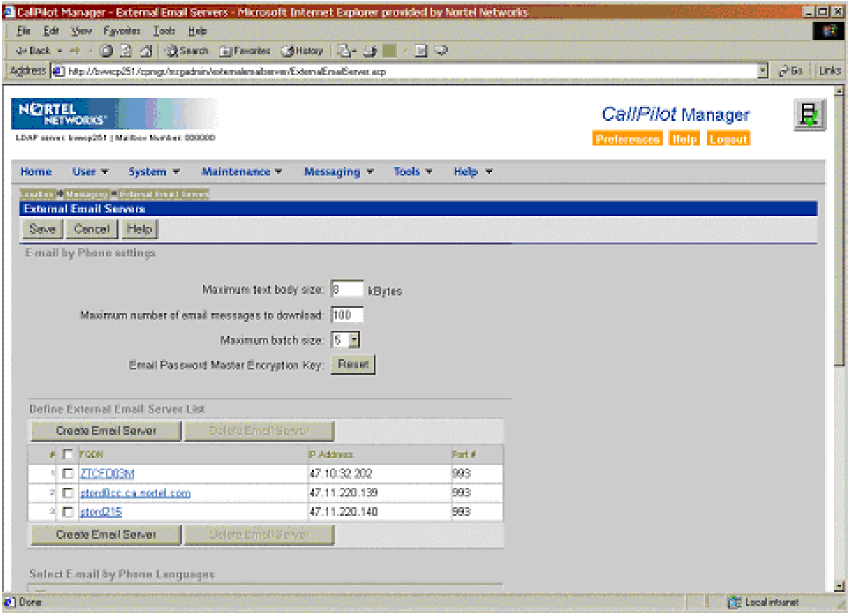
The procedures for configuring the Email-by-Phone feature are as follows:

- To configure the external e-mail server
- To configure the user’s class of service
- To configure the user’s e-mail account

To be able to execute the configuration procedures, you must be logged in to CallPilot Manager.

To configure the external e-mail server

1 In CallPilot Manager, choose Messaging → External E-mail Servers.


CallPilot Manager - External Email Servers - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go Links
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Save Cancel Help
Create Email Server
Delete Email Server
Done
Local intranet

External Email Servers

E-mail by Phone settings

Maximum text body size: 8 kBytes

Maximum number of email messages to download: 100

Maximum batch size: 5

Email Password Master Encryption Key: Reset

Define External Email Server List

#	□	FQDN	IP Address	Port #
1	□	ZTCFD03M	47.10.32.202	993
2	□	stcnd0cc.ca.nortel.com	47.11.220.139	993
3	□	stcnd215	47.11.220.140	993

Select E-mail by Phone Languages

2 Type an appropriate number in the Maximum text body size: text box. This is the size in kilobytes of the messages that the users are allowed to download and read. If the size of an e-mail message exceeds the maximum text body size, the e-mail message is truncated when downloaded to disk.

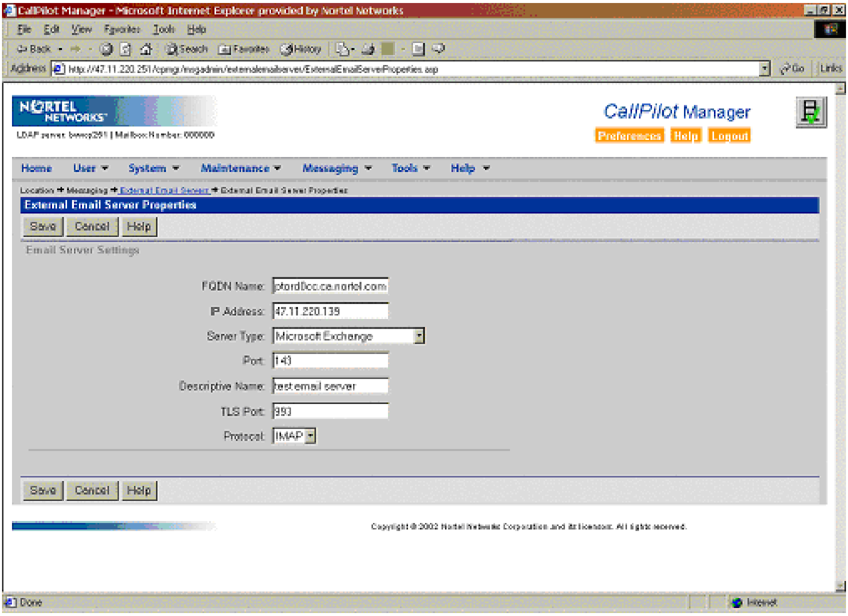
3 Type an appropriate number in the Maximum number of e-mail messages to download: text box. This is the number of e-mail messages that the user is allowed to download to disk.

Note: An e-mail message is downloaded only when a user presses the DTMF key “2” to play the message or the DTMF key “7-7” to print the message.

4 Select a number from the Maximum batch size: drop-down list. This is the maximum number of e-mail headers that the mailbox owner can retrieve once from the external e-mail server for review.

5 Click Create Email Server.

Result: The External Email Server Properties page is displayed.


CallPilot Manager - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47.11.220.251/cpmgr/msgadmin/externalemailserver/ExternalEmailServerProperties.asp
Go Links
NORTEL NETWORKS
LDAP server: bvwcp251 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location → Messaging → External Email Servers → External Email Server Properties
External Email Server Properties
Save Cancel Help
Email Server Settings
Save Cancel Help
Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.
Done
Internet

FQDN Name: ptord0cc.ca.nortel.com

IP Address: 47.11.220.139

Server Type: Microsoft Exchange

Port: 143

Descriptive Name: test email server

TLS Port: 993

Protocol: IMAP

6 Type the fully qualified domain name (FQDN) of the e-mail server in the FQDN Name: text box; for example, ptord0cc.ca.nortel.com.

7 Type the internet protocol (IP) address of the e-mail server in the IP Address: text box.

8 Choose the type of e-mail server from the Server Type: drop-down list; for example, Microsoft Exchange, Novell GroupWise or Lotus Notes.

9 Type 143 in the Port: text box. The port number for the Email-by-Phone feature must be 143.

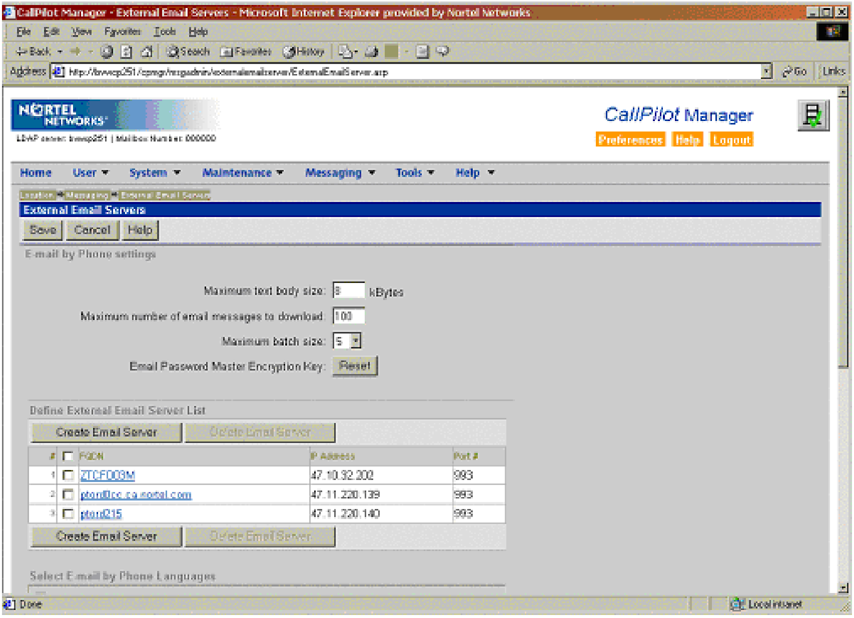
10 Type a name in the Descriptive Name: text box. The mailbox users identify the e-mail server with this name. You can type a maximum of 255 characters in this text box.

11 Type 993 in the TLS Port: text box. The TLS port number for the Email-by-Phone feature must be 993.

12 Choose IMAP from the Protocol: drop-down list. The IMAP protocol must be selected for the Email-by-Phone feature.

13 Click Save.

Result: The Email-by-Phone settings page is displayed.


CallPilot Manager - External Email Servers - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://bvwcp251/cpmgr/msgadmin/externalemailserver/ExternalEmailServer.asp
Go Links
NORTEL NETWORKS
LDAP server: bvwcp251 | Mailbox Number: 000000
CallPilot Manager
Preferences Help Logout
Home User System Maintenance Messaging Tools Help
Location Messaging External Email Server
External Email Servers
Save Cancel Help
Done
Local intranet

E-mail by Phone settings

Maximum text body size: 8 kBytes

Maximum number of email messages to download: 100

Maximum batch size: 5

Email Password Master Encryption Key: Reset

Define External Email Server List

Create Email Server | Delete Email Server

#	□	FQDN	IP Address	Port #
1	□	ZTCF003M	47.10.32.202	993
2	□	ptord0cc.ca.nortel.com	47.11.220.139	993
3	□	ptord215	47.11.220.140	993

Create Email Server | Delete Email Server

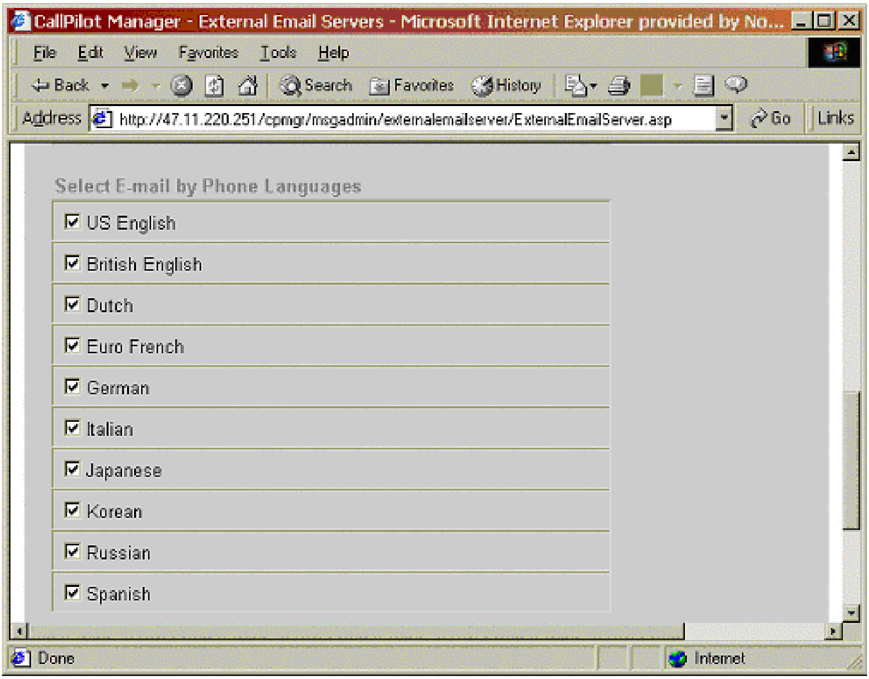
Select E-mail by Phone Languages

14 Click Reset to reset the e-mail password master encryption key.

Note: You can also reset the encryption key from a DOS window with the following command:
`D:\nortel\mpcx\bin\nmcrypt_updtkey.exe`.

15 Scroll down to the Select E-mail by Phone Languages page and select the check boxes corresponding to the languages that you want to be supported on the CallPilot server.

Note: You must select at least one language to enable the Email-by-Phone feature.



CallPilot Manager - External Email Servers - Microsoft Internet Explorer provided by No...
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47.11.220.251/cpmgr/msgadmin/externalemailserver/ExternalEmailServer.asp
Go Links
Done
Internet

Select E-mail by Phone Languages

☑ US English

☑ British English

☑ Dutch

☑ Euro French

☑ German

☑ Italian

☑ Japanese

☑ Korean

☑ Russian

☑ Spanish

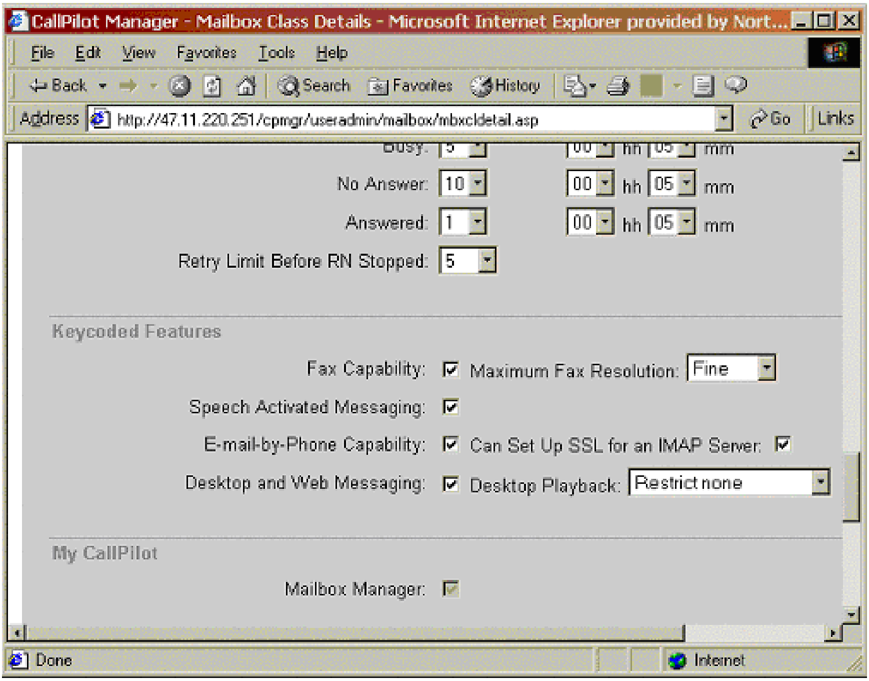
16 Click Save.

To configure the user’s class of service

1 In CallPilot Manager, choose Messaging → User → Mailbox Classes.

2 Double-click the mailbox class for which you want to enable the Email-by-phone feature.

Result: The Mailbox Call Details page is displayed.


CallPilot Manager - Mailbox Class Details - Microsoft Internet Explorer provided by Nort...
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
History
Address
http://47.11.220.251/cpmgr/useradmin/mailbox/mbxcldetail.asp
Go
Links
Done
Internet

Busy: 5 00 hh 05 mm

No Answer: 10 00 hh 05 mm

Answered: 1 00 hh 05 mm

Retry Limit Before RN Stopped: 5

Keycoded Features

Fax Capability: ☑ Maximum Fax Resolution: Fine

Speech Activated Messaging: ☑

E-mail-by-Phone Capability: ☑ Can Set Up SSL for an IMAP Server: ☑

Desktop and Web Messaging: ☑ Desktop Playback: Restrict none

My CallPilot

Mailbox Manager: ☑

3 Select the Fax Capability: check box if you want to enable the printing of e-mail messages.

4 Click Save.

To configure the user’s e-mail account

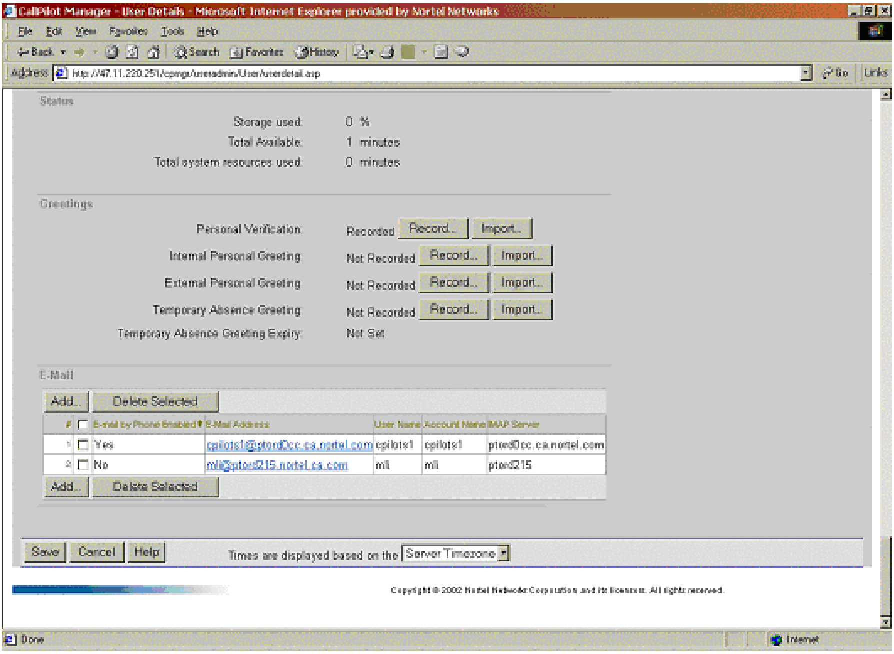
Before you begin

The administrator can enter the account information in CallPilot Manager, except the password. The users can enter their account information in My CallPilot using a valid password.

1 In CallPilot Manager, choose Messaging → User → User Search.

2 Double-click the name of the user for whom the account information is displayed.

Result: The User Details page is displayed.


CallPilot Manager - User Details - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47.11.220.251/cpmgr/useradmin/User/userdetail.asp
Go Links
Record... Import...
Add... Delete Selected
Save Cancel Help
Done
Internet

Status

Storage used: 0 %
Total Available: 1 minutes
Total system resources used: 0 minutes

Greetings

Personal Verification: Recorded
Internal Personal Greeting: Not Recorded
External Personal Greeting: Not Recorded
Temporary Absence Greeting: Not Recorded
Temporary Absence Greeting Expiry: Not Set

E-Mail

#	□	E-mail by Phone Enabled	E-Mail Address	User Name	Account Name	IMAP Server
1	□	Yes	cpilots1@ptordOcc.ca.nortel.com	cpilots1	cpilots1	ptordOcc.ca.nortel.com
2	□	No	mli@ptord215.nortel.ca.com	mli	mli	ptord215

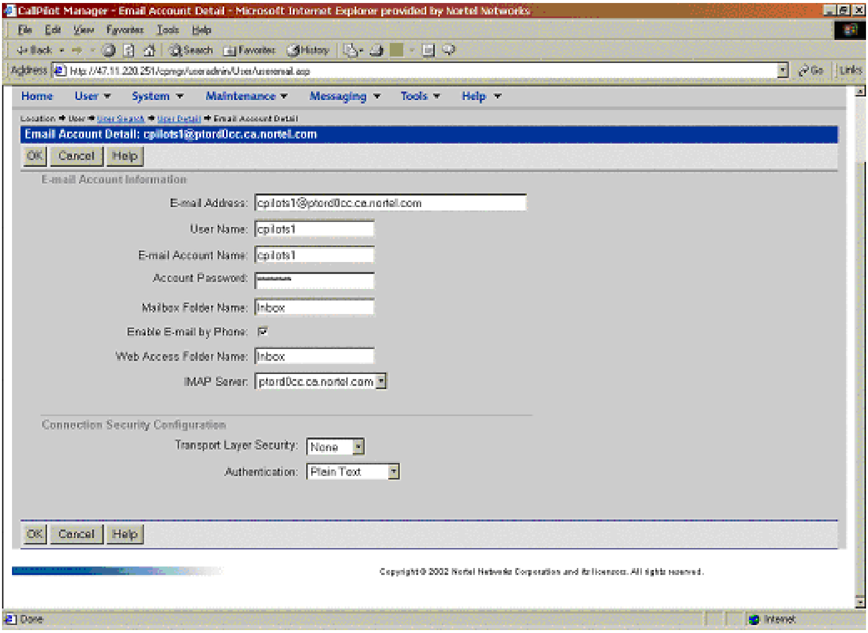
Times are displayed based on the Server Timezone

Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.

3 Scroll to the bottom of the User Details page.

4 Click Add to create an e-mail account.

Result: The Email Account Detail page is displayed.


CallPilot Manager - Email Account Detail - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47.11.220.251/cpmgr/useradmin/User/useremail.asp
Go Links
Home User System Maintenance Messaging Tools Help
Location ➔ User ➔ User Search ➔ User Detail ➔ Email Account Detail
OK Cancel Help
Done Internet
Copyright © 2002 Nortel Networks Corporation and its licensors. All rights reserved.

Email Account Detail: cpilots1@ptord0cc.ca.nortel.com

E-mail Account Information

E-mail Address: cpilots1@ptord0cc.ca.nortel.com

User Name: cpilots1

E-mail Account Name: cpilots1

Account Password: ********

Mailbox Folder Name: Inbox

Enable E-mail by Phone: ☑

Web Access Folder Name: Inbox

IMAP Server: ptord0cc.ca.nortel.com

Connection Security Configuration

Transport Layer Security: None

Authentication: Plain Text

5 Type the user's e-mail address in the E-mail Address: text box. You can type a maximum of 255 characters in this text box.

Tip: The server name in the e-mail address must be the e-mail server name selected in the IMAP Server: drop-down list.

6 Type the name of the mailbox owner in the User Name: text box. This is the name associated with the e-mail address and appears in the From: field of the e-mail messages received from the mailbox owner. You can type a maximum of 160 characters in this text box.

7 Type the user name in the E-mail Account Name: text box. This is the name that the mailbox owner uses to log in to the e-mail server. You can enter a maximum of 80 characters in this text box.

8 The password required to log in to the e-mail server must be entered in the Account Password: text box. The password can contain a maximum of 80 characters. Enter information in this text box as follows:

- **a.** Type the user’s password if you know it.
- **b.** Type an x if you do not know the user’s password.

Note: After the e-mail account is configured, the mailbox owner must enter a valid e-mail account password in My CallPilot to be able to access the Email-by-Phone feature.

9 Type in the Mailbox Folder Name: text box the name of the e-mail server folder accessible when the mailbox owner uses Email-by-Phone. The folder must already exist on the e-mail server. The folder name can contain a maximum of 80 characters.

Example: These are examples of common folder names: Inbox, Sent items and Drafts.

10 Select the Enable E-mail by Phone check box to enable the Email-by-Phone feature for the user’s account.

11 Type in the Web Access Folder Name: text box the name of the folder that is accessible when the mailbox owner uses Web Messaging. The folder name can contain up to 50 characters.

Example: These are examples of common folder names: Inbox, Sent items and Drafts.

12 Select the server associated with the e-mail account in the IMAP Server: drop-down list.

13 Specify the security options for the e-mail account in the Connection Security Configuration section:

- **a.** Select an encryption protocol for data transmission from the Transport Layer Security: drop-down list. Select the None option if you want to disable the encryption for the e-mail account.
- **b.** Select and authentication method for logging in to the e-mail server from the Authentication: drop-down list. Select the None option if you want to disable the authentication for the e-mail account.

Note: The e-mail server associated with the e-mail account must support the selected security options.

14 Click OK.

Result: The User Details page is displayed.

15 Click Save. If you do not click Save, all the information entered for the user account is lost.

Note: If a valid e-mail account password was entered in step 8 and all the information has been provisioned correctly, the mailbox user is able to retrieve e-mail messages after the completion of this procedure.

Configuring Email-by-Phone using My CallPilot

Once the administrator provisioned the e-mail server using CallPilot Manager, the mailbox owner can configure the Email-by-Phone feature using My CallPilot. The My CallPilot server establishes its own connection with the configured e-mail servers when sending and receiving e-mail messages.

The CallPilot server provides the Email-by-Phone functionality. The mailbox owner uses My CallPilot to choose an e-mail account to set up as an Email-by-Phone account.

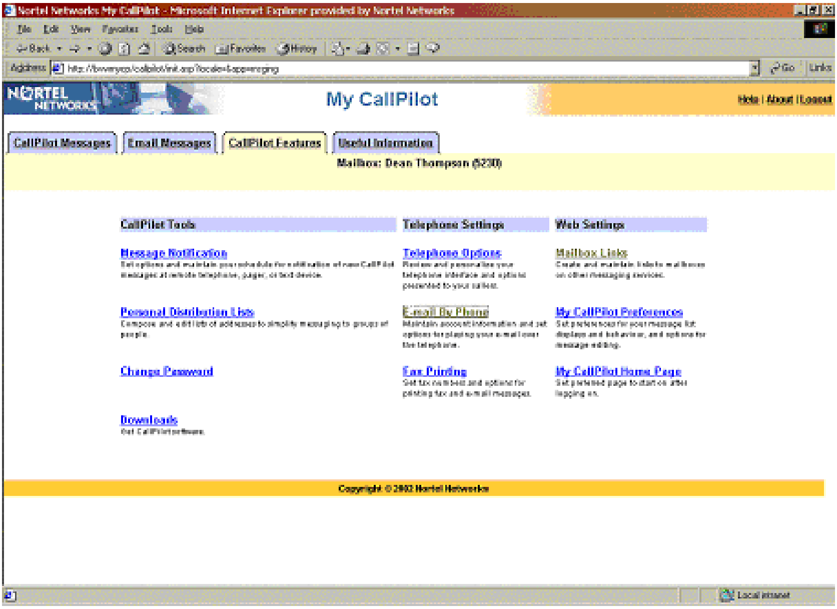
To configure an e-mail account

Before you begin

To be able to execute the procedures you must be logged in to My CallPilot.

1 In My CallPilot, click the CallPilot Features tab.

Result: The CallPilot Features page is displayed.


Nortel Networks My CallPilot - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go Links
NORTEL NETWORKS
My CallPilot
Help | About | Logout
CallPilot Messages
Email Messages
CallPilot Features
Useful Information
Local intranet

Mailbox: Dean Thompson (6230)

CallPilot Tools

Message Notification
Set options and maintain your schedule for notification of new CallPilot messages at remote telephone, pager, or text device.

Personal Distribution Lists
Compose and edit lists of addresses to simplify messaging to groups of people.

Change Password

Downloads
Get CallPilot software.

Telephone Settings

Telephone Options
Review and personalize your telephone interface and options presented to your callers.

E-mail By Phone
Maintain account information and set options for playing your e-mail over the telephone.

Fax Printing
Set fax numbers and options for printing fax and e-mail messages.

Web Settings

Mailbox Links
Create and maintain links to mailboxes on other messaging services.

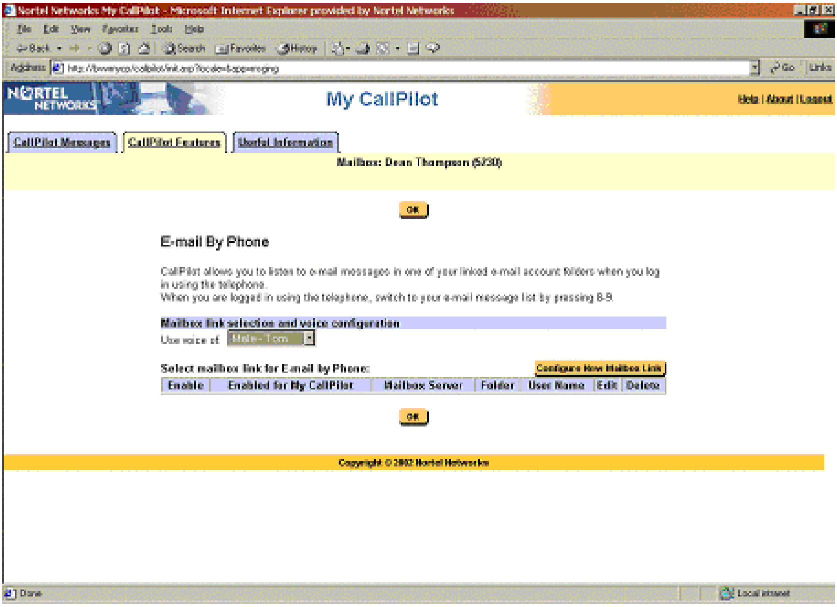
My CallPilot Preferences
Set preferences for your message list displays and behavior, and options for message editing.

My CallPilot Home Page
Set preferred page to start on after logging on.

Copyright © 2002 Nortel Networks

2 Click Email-by-Phone.

Result: The Email-by-Phone page is displayed.



Nortel Networks My CallPilot - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go Links
My CallPilot
Help | About | Logout
CallPilot Messages
CallPilot Features
Useful Information
OK
Done
Local intranet

Mailbox: Dean Thompson (5730)

E-mail By Phone

CallPilot allows you to listen to e-mail messages in one of your linked e-mail account folders when you log in using the telephone.
When you are logged in using the telephone, switch to your e-mail message list by pressing 8-9.

Mailbox link selection and voice configuration

Use voice of Male - Tom

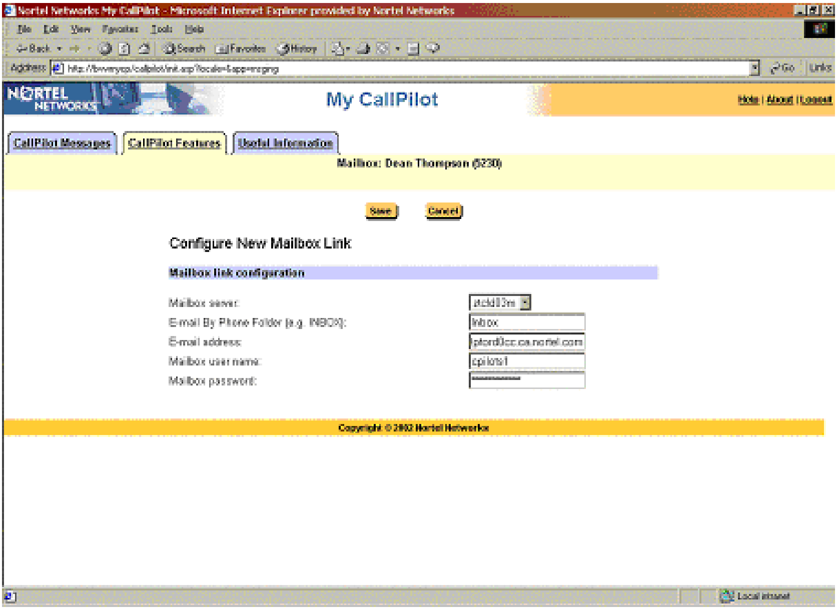
Select mailbox link for E-mail by Phone: Configure New Mailbox Link

Enable	Enabled for My CallPilot	Mailbox Server	Folder	User Name	Edit	Delete

Copyright © 2002 Nortel Networks

3 Click Configure New Mailbox Link.

Result: The Configure New Mailbox Link page is displayed.


Nortel Networks: My CallPilot - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go Links
NORTEL NETWORKS
My CallPilot
Help | About | Logout
CallPilot Messages
CallPilot Features
Useful Information
Save
Cancel
Copyright © 2002 Nortel Networks
Local intranet

Mailbox: Dean Thompson (5230)

Configure New Mailbox Link

Mailbox link configuration

Mailbox server: ztcfd03m

E-mail By Phone Folder (e.g. INBOX): Inbox

E-mail address: ptord0cc.ca.nortel.com

Mailbox user name: cpilots1

Mailbox password: ***********

4 Select the appropriate e-mail server for your e-mail account from the Mailbox server: drop-down list; for example, ztcfd03m.

5 Type in the E-mail By Phone Folder (e.g. INBOX): text box the name of the e-mail folder for which you want to use the Email-by-Phone feature.

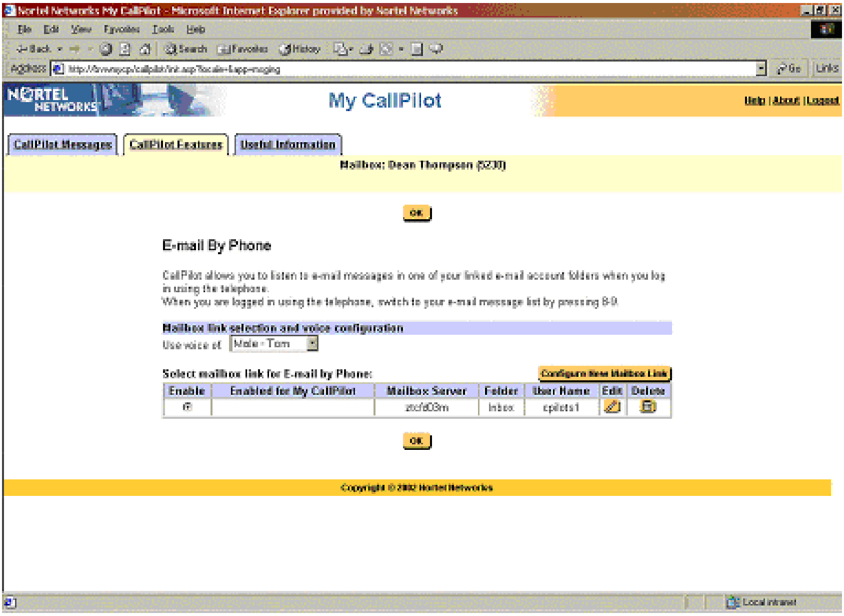
6 Type your e-mail address in the E-mail address: text box; for example, cpilots1@ptord0cc.ca.nortel.com.

7 Type your e-mail user name in the Mailbox user name: text box; for example, cpilots1. The e-mail user name is the ID that you use to log in to the e-mail server.

8 Enter the e-mail account password in the Mailbox password: text box.

9 Click Save.

Result: The Email-by-Phone page is displayed again.



Nortel Networks My CallPilot - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http:// /mycp/callpilot/link.asp?locale=&app=maging
Go Links
NORTEL NETWORKS
My CallPilot
Help | About | Logout
CallPilot Messages
CallPilot Features
Useful Information
OK
Configure New Mailbox Link
OK
Local intranet

Mailbox: Dean Thompson (5230)

E-mail By Phone

CallPilot allows you to listen to e-mail messages in one of your linked e-mail account folders when you log in using the telephone.
When you are logged in using the telephone, switch to your e-mail message list by pressing 8-9.

Mailbox link selection and voice configuration

Use voice of: Male - Tom

Select mailbox link for E-mail by Phone:

Enable	Enabled for My CallPilot	Mailbox Server	Folder	User Name	Edit	Delete
●		zrcfd03m	Inbox	cpilots1	✎	🗑

Copyright © 2002 Nortel Networks

10 Click OK.

Result: You can now log in to the CallPilot mailbox, press the DTMF keys “8-9” and start an Email-by-Phone session.

Troubleshooting Email-by-Phone

General

This section is intended to assist technical support personnel in troubleshooting Email-by-Phone issues. The following list presents the Email-by-Phone issues in the order of their importance and frequency:

- the configuration of the e-mail server and of the user e-mail account is incorrect
- the Email-by-Phone feature cannot connect to the external e-mail server
- the known Email-by-Phone feature limitations in CallPilot 2.0

Configuration issues

Configuration issues can cause various types of problems, such as the following:

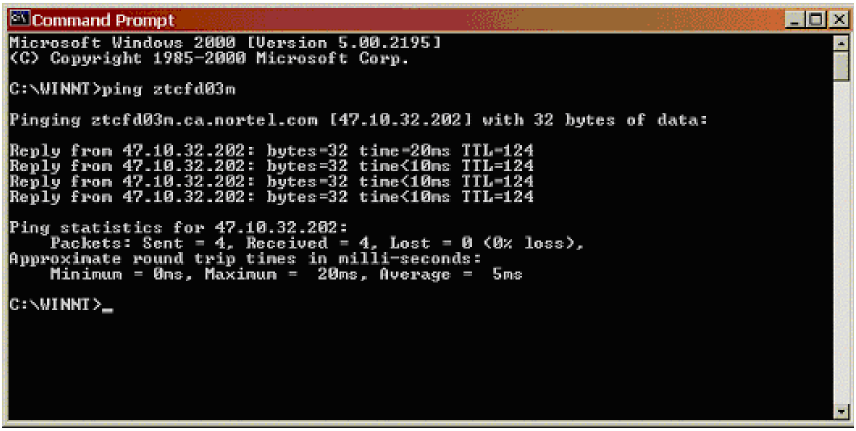
- the user cannot log in to the e-mail server for an Email-by-Phone session
- the user cannot play a particular e-mail message
- the user reports that the e-mail message list is always empty

The first step when troubleshooting any Email-by-Phone issue is to check the configuration settings in CallPilot Manager. Go through the procedures given in “Configuring Email-by-Phone” on page 428 and make sure that all the information is known and properly entered. If the configuration is correct and the Email-by-Phone feature still does not function properly, proceed with the next troubleshooting action that is likely to solve the problem.

User cannot connect to the external e-mail server

To troubleshoot this Email-by-Phone issue, proceed as follows:

1. Ensure that the Email-by-Phone configuration is correct.
2. Verify the connection to the external e-mail server. To do this, ping from the CallPilot server the external e-mail server to which the user tried to connect. At the DOS command line, type `ping <external e-mail server name>`; for example, `ping ztcfd03`, as shown in the following illustration.

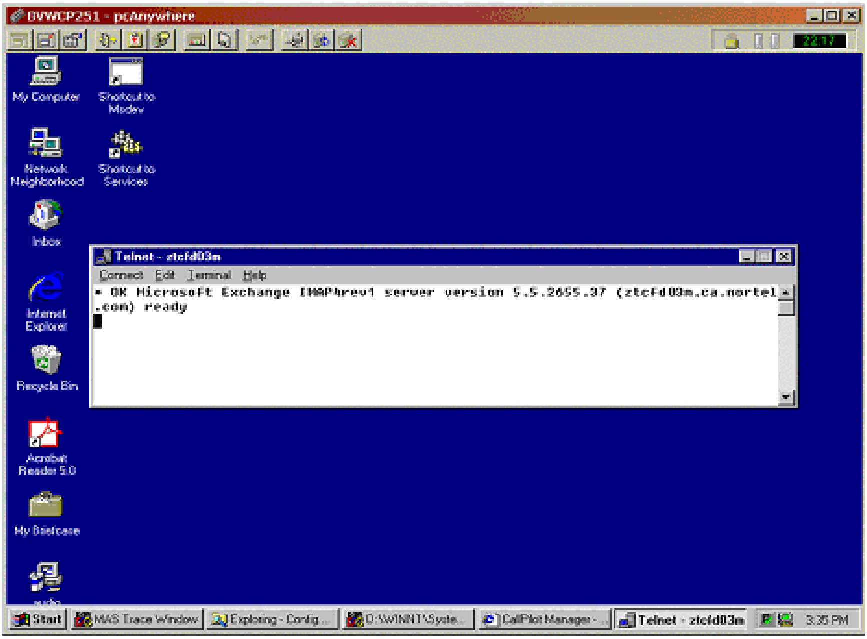
   

   ```
   Microsoft Windows 2000 [Version 5.00.2195]
   (C) Copyright 1985-2000 Microsoft Corp.

   C:\WINNT>ping ztcfd03m

   Pinging ztcfd03m.ca.nortel.com [47.10.32.202] with 32 bytes of data:

   Reply from 47.10.32.202: bytes=32 time=20ms TTL=124
   Reply from 47.10.32.202: bytes=32 time<10ms TTL=124
   Reply from 47.10.32.202: bytes=32 time<10ms TTL=124
   Reply from 47.10.32.202: bytes=32 time<10ms TTL=124

   Ping statistics for 47.10.32.202:
       Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
       Minimum = 0ms, Maximum =  20ms, Average =  5ms

   C:\WINNT>_
   ```

   The ping command does not show any points of failure between the CallPilot server and the external e-mail server, but indicates if a connection between the CallPilot server and the e-mail server exists through the network.

3. Depending on the result of the ping command, proceed as follows:

   a. If the ping command shows that a connection is present between the CallPilot server and the external e-mail server, try to log in to the IMAP port of the external e-mail server. In a DOS command window, type `telnet <external e-mail server name> 143`; for example, `telnet ztcfd03 143`, where `ztcfd03` is the external e-mail server name. If a connection between the CallPilot server and the e-mail server exists, a Telnet window indicating that the e-mail server is ready appears on the screen.



```
* OK Microsoft Exchange IMAP4rev1 server version 5.5.2655.37 (ztcfd03m.ca.nortel
.com) ready
```

If a window indicating that the server is not ready appears on the screen, then a network issue affects the connection to the e-mail server.

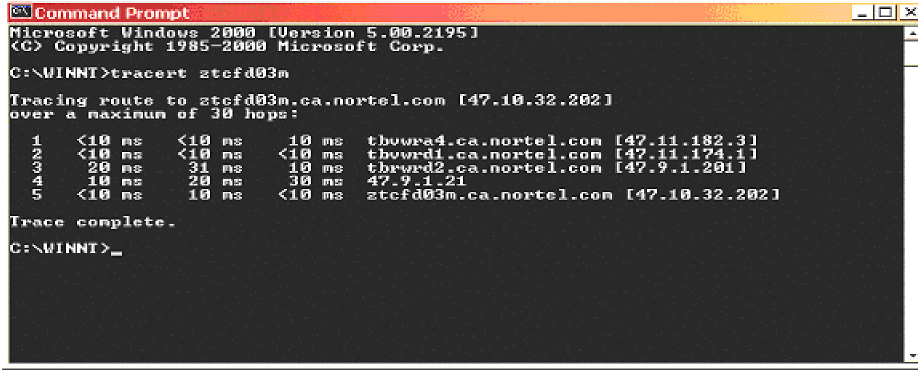
b. If the ping command indicated no connection between the CallPilot server and the external e-mail server, go to step 6.

4 If the Telnet window indicates that the e-mail server is ready, try to log in to this server by typing the following command: `001 login <user ID> <user password>`. The following message indicates that the attempt to log in to the e-mail server was successful: `001 OK Login completed`.

Note: If the previous message does not appear, then the user ID or the password is not correct.

5 Log out from the e-mail server by typing `002 logout`.

6 If the ping command indicated no connection between the CallPilot server and the external e-mail server, use the trace route command to detect subnet type issues. In the DOS command window on the CallPilot server, type `tracert <external e-mail server name>`.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT>tracert ztcfd03m

Tracing route to ztcfd03m.ca.nortel.com [47.10.32.202]
over a maximum of 30 hops:

  1    <10 ms   <10 ms    10 ms  tbvwra4.ca.nortel.com [47.11.182.3]
  2    <10 ms   <10 ms   <10 ms  tbvwrd1.ca.nortel.com [47.11.174.1]
  3     20 ms    31 ms    10 ms  tbrwrd2.ca.nortel.com [47.9.1.201]
  4     10 ms    20 ms    30 ms  47.9.1.21
  5    <10 ms    10 ms   <10 ms  ztcfd03m.ca.nortel.com [47.10.32.202]

Trace complete.

C:\WINNT>_
```

The `tracert <external e-mail server name>` command traces the route to the external e-mail server and identifies any points of failure.

Known Email-by-Phone feature limitations in CallPilot 2.0

The Email-by-Phone feature can be used only if the external e-mail server supports the IMAP r4 protocol. The Email-by-Phone feature has been tested with the following e-mail servers:

- Microsoft Exchange 5.5
- Novell GroupWise 5.5 and 6.0
- Lotus Notes Domino

The following are the Email-by-Phone feature limitations in CallPilot 2.0:

- The E-mail-by-Phone feature supports only server-based folders.
  - The e-mail folder that the user accesses by way of Email-by-Phone must reside on the e-mail server.
  - The E-mail-by-Phone feature cannot access e-mail messages stored in a shared directory on a network or on a personal computer.
- The E-mail-by-Phone feature supports only the text body of the e-mail messages, not the attachments.

- The E-mail-by-Phone feature does not support the following commands:
  - Compose
  - Reply
  - Reply All
  - Forward

User cannot play a particular e-mail message

If a user reports that a particular e-mail message cannot be played using the Email-by-Phone features, follow these steps.

Ensure that all required CallPilot PEPs have been applied. The PEP CP20126G053S is specific to the Email-by-Phone feature. This PEP requires that the CallPilot server be updated to SU-01. Go to the Meridian PEP library (MPL) Web site to find the most recent updates.

Make sure that all 10 supported languages are selected on the Select E-mail by Phone Languages page, as indicated in “To configure the external e-mail server” on page 429, if the user cannot play messages in one particular language.

Check the source of the e-mail message in Outlook Express and verify if the message is encoded with a text encoding standard that the Email-by-Phone feature supports:

- ISO-8859-1—the Email-by-Phone feature supports the playing of e-mail messages in the following languages: English, French, German, Spanish, Italian, and Dutch.
- UTF-8—the Email-by-Phone feature supports the playing of e-mail messages in the following languages: English, French, German, Spanish, Italian, Dutch, Russian, Korean, and Japanese.

To check the source of an e-mail message in Outlook Express, proceed as follows:

1 Open the e-mail message that failed to play.

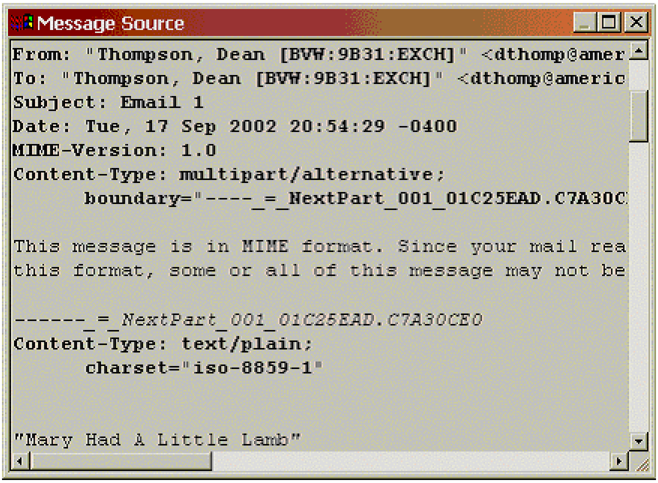
2 Choose File → Properties.

Result: The Properties window is displayed.

3 Click the Details tab.

4 Click Message Source.

Result: The Message Source window appears.



```
From: "Thompson, Dean [BVW:9B31:EXCH]" <dthomp@amer
To: "Thompson, Dean [BVW:9B31:EXCH]" <dthomp@americ
Subject: Email 1
Date: Tue, 17 Sep 2002 20:54:29 -0400
MIME-Version: 1.0
Content-Type: multipart/alternative;
      boundary="----_=_NextPart_001_01C25EAD.C7A30C

This message is in MIME format. Since your mail rea
this format, some or all of this message may not be

------_=_NextPart_001_01C25EAD.C7A30CE0
Content-Type: text/plain;
      charset="iso-8859-1"


"Mary Had A Little Lamb"
```

5 Verify if the character set of the e-mail message is supported by the Email-by-Phone feature. In this example, the line that provides information about the character set is `charset="iso-8859-1"`.

Empty e-mail message list

If a user reports that the e-mail message list is empty, verify if the e-mail folder that the user tries to access resides on the e-mail server. As indicated in “Known Email-by-Phone feature limitations in CallPilot 2.0” on page 445, the e-mail message folder that the user can access by way of the Email-by-Phone feature must reside on the e-mail server and not on the user’s PC. Also make sure that the name of the folder that the user tries to access is correct.

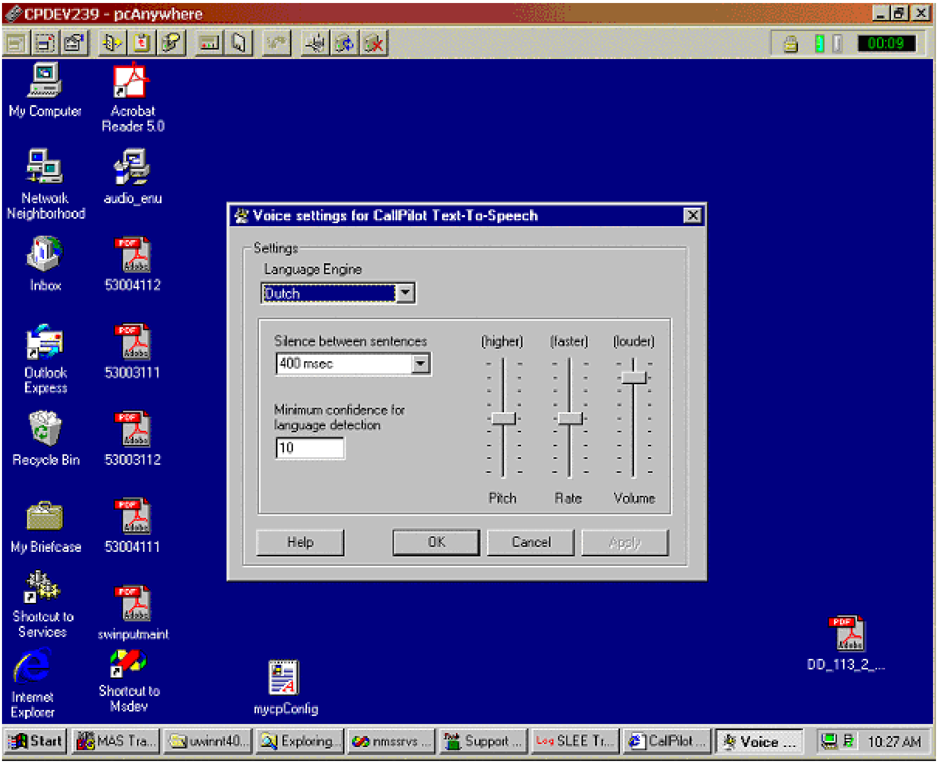
Customizing playback controls

To adjust TTS settings

You must use the text-to-speech (TTS) engine setting tool to make playback adjustments to each of the languages that the Email-by-Phone feature supports.

1 Choose Start → Programs → CallPilot → System Utilities → TTS Engine Settings.

Result: The Voice settings for CallPilot Text-To-Speech window opens.



Voice settings for CallPilot Text-To-Speech

Settings

Language Engine: Dutch

Silence between sentences: 400 msec

Minimum confidence for language detection: 10

2 Select from the Language Engine drop-down list the language for which you want to adjust the playback settings.

3 Select a convenient duration for the silence periods between sentences from the Silence between sentences drop-down list. The available silence duration options range from 0 msec through 1800 msec.

4 Adjust the pitch of the sound of the user-defined speaker using the Pitch slider.

5 Adjust the speed at which the message is read using the Rate slider.

6 Adjust the volume of the user-defined speaker as desired using the Volume slider.

Note: The Minimum confidence for language detection setting is not used at this time. Nortel Networks software performs the language detection.

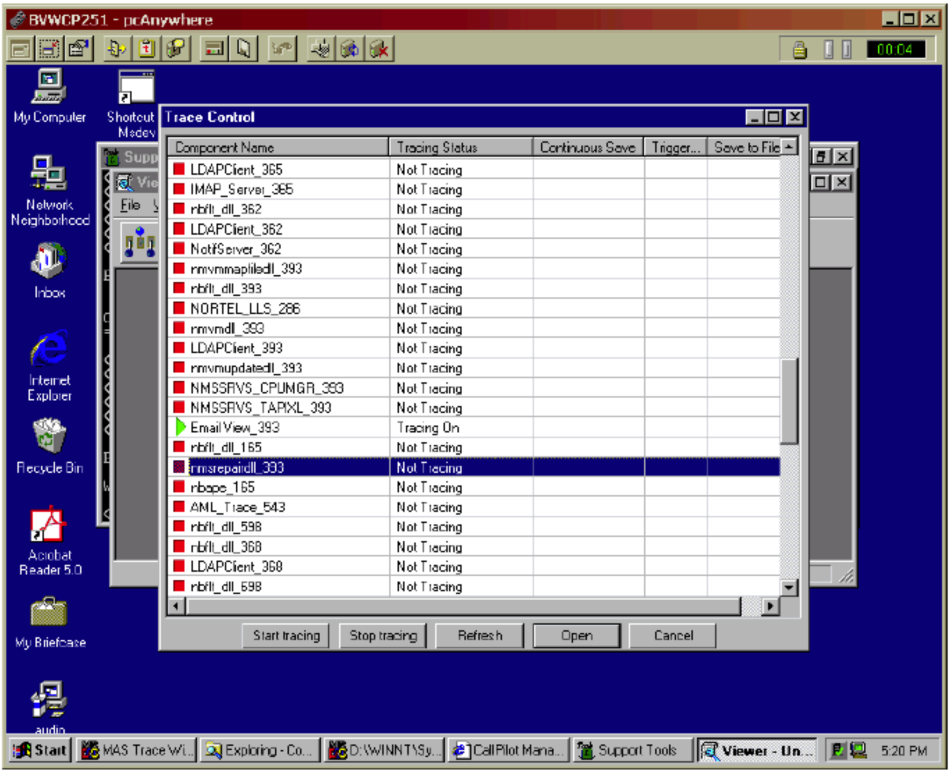
Tracing an Email-by-Phone session

A CallPilot support tool has been developed to obtain detailed tracing of an Email-by-Phone session. Follow this procedure to trace an Email-by-Phone session.

To trace an Email-by-Phone session

1 Choose CallPilot support tools → 9 (Call Processing Utilities) → 3 (Trace Viewer).

Result: The Trace Control window appears.



Component Name	Tracing Status	Continuous Save	Trigger...	Save to File
🟥 LDAPClient_365	Not Tracing			
🟥 IMAP_Server_365	Not Tracing			
🟥 nbflt_dll_362	Not Tracing			
🟥 LDAPClient_362	Not Tracing			
🟥 NotifServer_362	Not Tracing			
🟥 nmvmmapfiledll_393	Not Tracing			
🟥 nbflt_dll_393	Not Tracing			
🟥 NORTEL_LLS_286	Not Tracing			
🟥 nmvmdll_393	Not Tracing			
🟥 LDAPClient_393	Not Tracing			
🟥 nmvmupdatedll_393	Not Tracing			
🟥 NMSSRVS_CPUMGR_393	Not Tracing			
🟥 NMSSRVS_TAPIXL_393	Not Tracing			
▶ EmailView_393	Tracing On			
🟥 nbflt_dll_165	Not Tracing			
🟥 nmsrepairdll_393	Not Tracing			
🟥 nbape_165	Not Tracing			
🟥 AML_Trace_543	Not Tracing			
🟥 nbflt_dll_598	Not Tracing			
🟥 nbflt_dll_368	Not Tracing			
🟥 LDAPClient_368	Not Tracing			
🟥 nbflt_dll_698	Not Tracing			

2 Double-click the session with the highest process number (EmailView_393 in this example) in the Component Name column.

3 Start an Email-by-Phone session.

Result: Trace text similar to the following appears in your window.

```
Nov 28, 2001   11:57:37:297  18150   8    3    N/A   StartSession: Entering

Nov 28, 2001   11:57:37:307  18150   8    3    N/A   AddRequest: Entering

Nov 28, 2001   11:57:37:307  18150   8    3    N/A   AddRequest: Exiting OK

Nov 28, 2001   11:57:37:307  18150   8    3    N/A   StartSession: Exiting OK

Nov 28, 2001   11:57:37:317  18150   8    3    N/A   RunThread: Event in
request queue

Nov 28, 2001   11:57:37:317  18150   8    3    N/A   ProcessRequest: Entering

Nov 28, 2001   11:57:37:317  18150   8    2    N/A   ProcessRequest: Request
of type 1

Nov 28, 2001   11:57:37:317  18150   8    2    N/A   PerformStartupLDAP:
Entering

Nov 28, 2001   11:57:38:328  18150   8    3    N/A   PerformStartupLDAP:

About to login to IMAP server

Nov 28, 2001   11:57:38:328  18150   8    3    N/A   Email Login:FQ Domain

Name:ptord0cc.ca.nortel.comIP Address:47.11.8.14  Account Name: cpilots1
Password: PrivateSSL: NoPort

Nov 28, 2001   11:57:38:328  18150   8    3    N/A   PerformStartupLDAP:

About to call IMAP Logon

Nov 28, 2001   11:57:38:629  18150   8    3    N/A   PerformStartupLDAP:

IMAP Logon succeeded

Nov 28, 2001   11:57:38:649  18150   8    3    N/A   PerformStartupLDAP:
```

```
About to open user’s folder

Nov 28, 2001   11:57:38:709  18150   8    3    N/A   PerformStartupLDAP:

About to call DownloadHeader

Nov 28, 2001   11:57:38:709  18150   8    3    N/A   PerformStartupLDAP:

Invoking callback with tReply.iStatus=59422

Nov 28, 2001   11:57:38:709  18150   8    3    N/A   PerformStartupLDAP:

Exiting OK
```

Note: The Nortel Networks support team can interpret the trace information.

Part 6

Monitoring the CallPilot system

In this part

Chapter 22

Monitoring the CallPilot server and resources

In this chapter

Section A: Monitoring the CallPilot server performance

In this section

Viewing the performance of CallPilot server

Introduction

To view the performance of CallPilot server, in the System menu, click Performance Monitor.

Performance Monitor updates the following information about the CallPilot server every 10 seconds.

Column	Description
Time and Date	The time and date on the server when server performance was sampled.
% Processor Usage	The percentage of processor capacity being used. This figure fluctuates according to the number and type of events that are running on the server.
Free RAM (Bytes)	The amount of memory that is available on the server, in bytes.
% Free Disk Space	The percentage of free disk space on each of the CallPilot server’s fixed disks.

Finding information about the CallPilot server

Introduction

You may need Server Settings information when you communicate with product support personnel.

The Server Settings information includes

- list of features and services installed on the CallPilot server
- resource list showing the capacity of the CallPilot server
- description of the switch connected to the CallPilot server
- serial port settings of the CallPilot server

Viewing server settings

To view CallPilot server settings, in the System menu, click Server Settings.

Determining the capacity of the CallPilot server

Use the Server Settings page to find information such as

- the server version, switch type, and platform type
- channel allocations
- maximum number of mailboxes, and the maximum number that can be allocated to voice, fax or speech recognition functionality
- system prompt, e-mail by phone, and speech recognition languages
- maximum number of mailbox storage hours the system can support
- maximum number of NMS locations, networking sites, and DSPs the system can support

Listing the applications and services installed on the CallPilot server

If you are not sure whether a particular application or service is installed on a CallPilot server, use the Server Settings page to display a list.

Finding information about the connected switch

Use the Server Settings page to display switch information such as

- the switch type (for example Meridian 1 or Succession CSE 1000) and sub-type (for example, Option 11C)
- the software release
- the IP address

Determining the CallPilot server serial port settings

Use the Server Settings page to display serial port configuration information such as

- port type
- baud rate
- data bits
- parity
- stop bits
- flow control

Running system reports

Introduction

The CallPilot Reporter feature provides the tools you need to run system status reports.

Use CallPilot Manager to configure the report data to collect. The administrator shortcuts on the CallPilot Manager home page provide a link to the Reporter program.

Collecting report data

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 CallPilot Reporter.

CallPilot collects OM data on the OM server in one hour intervals. Reporter then retrieves the data and stores it in the Reporter database.

To generate reports, OM data collection must be enabled. 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.

The storage period for the Reporter database is configured in Reporter. Refer to the Reporter online Help for more information.

Running reports

The Reporter utility provides predefined reports to help you monitor service usage and performance.

System status reports

These reports include data such as the number of callers who waited for a channel and the number of callers who abandoned their calls.

Run the following reports to view statistics for each channel type.

- Service Quality Summary report
- Service Quality Detail report
- Channel Usage report

Traffic reports

Run the System Traffic Summary report to identify how much particular services are used. For example, you can identify the percentage of total traffic generated by a service. This gives you an idea of whether the current channel allocations for that service are adequate.

Reports on deliveries to external DNs

You can view the average and maximum times that each service had to wait to acquire a channel.

Run the following reports to determine if services that deliver messages to external DNs are able to acquire channels when needed.

- DTT Activity report
- Fax Deliveries Activity report
- Fax on Demand Audit Trail Detail report
- Fax Print Audit Trail Detail report
- RN Activity report
- RN Audit Trail Detail report

Networking reports

If the AMIS or VPIM Networking services are installed, you can run the Open Networking Activity report. A high number of blocked sessions means that the service cannot acquire channels to complete calls.

Section B: Monitoring channels

In this section

Monitoring call channels

Introduction

If the CallPilot server has trouble processing incoming calls, use Channel Monitor to view the state of call channels.

From Channel Monitor, you can:

- monitor the current activity of functioning call channels, and identify which call channels are not functioning
- identify a call channel’s physical location

You can identify a channel’s physical location by its icon’s position on the Channel Monitor page. Channel Monitor also displays a channel's directory number (DN) and position (Label) in a popup when you move the mouse cursor over the channel's check box.

Changing the Channel Monitor refresh rate

By default, the Channel Monitor refreshes the display every five seconds with updated channel status information. Increasing the frequency of updates increases the load on the server.

Starting call channels

Starting an Off Duty call channel puts it into Idle state. Typically, you start call channels after the system has been powered up following major upgrades or installations. If a call channel is off duty for any other reason, use Channel Monitor to help you isolate the cause of the problem and take appropriate action to fix it. For example, you can run diagnostics on the call channel to check whether there is a problem with the call channel.

Call channel states

ATTENTION

After completing call processing, a channel remains in the active state in anticipation of receiving future calls. If it does not receive another call after 30 seconds, an active channel will change to an idle state.

The icon that appears for each channel indicates the channel status.

	Active		Off Duty
	Disabled		Power Off
	Idle		Remote (Yellow) Alarm
	In Test		Remote Off Duty
	Loading		Shutting Down
	Local (Red) Alarm	?	Uninitialized
	No Resources	🟦	ACCESS channel
	Not Configured	🟩	IVR channel

Looking up procedures in CallPilot Manager online Help

Find procedures for monitoring, starting, stopping, and troubleshooting call channels by looking up **channels** in the online Help Index.

Monitoring multimedia channels

Introduction

If the server experiences trouble processing incoming calls, you can view the state of voice, fax, and speech recognition channels in Multimedia Monitor.

From Multimedia Monitor, you can:

- monitor the current activity of functioning call channels, and identify which call channels are not functioning
- identify a call channel’s physical location
- identify the media type associated with a channel (voice, fax, or speech recognition) and review multimedia resources allocation

An understanding of channel allocation can help you determine if you must reconfigure the channels or add MPC-8 cards to increase the multimedia processing capacity of the server.

You can identify a channel’s physical location by its position on the Multimedia Monitor page. Multimedia Monitor also displays a channel's directory number (DN) and position (Label) in a pop-up when you move the mouse cursor over the channel's check box.

Changing the Multimedia Monitor refresh rate

By default, the Multimedia Monitor refreshes the display every five seconds with updated channel status information. Increasing the frequency of updates increases the load on the server.

Stopping multimedia channels

You can courtesy stop or stop channels to put them into Off Duty status. In Off Duty state, multimedia channels cannot carry any voice, fax, or speech recognition data.

ATTENTION

If you take multimedia channels off duty, you must manually start them in order to put them back on duty. Channels that have been manually taken off duty do not automatically start when the CallPilot server is restarted or powered up.

Starting off-duty multimedia channels

Starting an Off Duty channel puts it into the Idle state.

Typically, you start multimedia channels after the system has been powered up following major upgrades or installations.

If a multimedia channel is Off Duty for any other reason, you must isolate the cause of the problem and take appropriate action to fix it. For example, you can run diagnostics on the multimedia channel to determine if there is a problem with it.

Note: The Maintenance page appears only if it is possible to run diagnostics on the selected hardware.

Multimedia channel states

ATTENTION

After completing call processing, a channel remains in the active state in anticipation of receiving future calls. If it does not receive another call after 30 seconds, an active channel will change to an idle state.

The icon that appears for each channel indicates the channel status.

	Active		Not Configured
	Disabled		Off Duty
	Idle		Power Off
	In Test		Shutting Down
	Loading	?	Uninitialized
	No Resources		

Looking up procedures in CallPilot Manager online Help

Find procedures for monitoring, starting, stopping, and troubleshooting multimedia channels by looking up **channels** in the online Help Index.

Section C: Monitoring disk space

In this section

Monitoring Nortel directory disk space

Introduction

To monitor the disk space available for the Nortel directory, you must wait for alarms to be raised. You can, however, determine how much free space exists on this disk using the Server Performance Monitor (SPM).

For information on how to use the Server Performance Monitor, see Section A: “Monitoring the CallPilot server performance,” on page 459.

Alarms

Although you can use the SPM to monitor the Nortel directory disk space, alarms are raised if logical disk space becomes limited. Different alarms are raised depending on how much disk space is left on the logical drives.

Alarm	Amount of space left
Major	less than 10%
Critical	less than 5%

Monitoring Multimedia File System volumes

Introduction

The MMFS volumes store all voice and fax messages and other related multimedia files, such as user mailboxes, greetings, voice prompts, and voice menus. The server can have more than one volume, depending on the overall capacity of the system to process calls. When an MMFS volume is full, no new files can be created on that volume.

If an MMFS volume has less than 10 percent of disk space left, you must free up enough space to clear the alarms.

Note: When you lower the retention period for user messages you do not affect the database. You must be clear about which parts of the hard disk (either the database or the MMFS) are approaching a point where they are nearly full.

What monitoring MMFS volumes involves

Monitoring MMFS volumes involves waiting for alarms to be raised as available disk space becomes limited. You can, however, display or print reports on MMFS volume disk usage using Reporter. These reports indicate disk space usage patterns, which can help you to plan a strategy to deal with limited disk space.

Alarms

Although you can use Reporter to monitor MMFS volumes, alarms are raised as MMFS volumes fill up. Different alarms are raised, depending on how much disk space is left for the MMFS volume.

Alarm	Amount of space left
Major	less than 10%
Critical	less than 5%

When alarms are raised, a warning box appears indicating the volume ID and the percentage full.

Clearing alarms

Alarms are cleared when less than 88 percent of MMFS volume disk space is being used. To clear alarms, you must free up space on the MMFS volume for which the alarm was raised.

- If one MMFS volume is full while other volumes are empty, you can move users' mailboxes from the full volume to another one.
- Disk space usage patterns on voice mail systems fluctuate, because voice messages are constantly created and deleted. If all volumes are filling up, you can do the following actions to reduce the size of mailboxes:
  - Send a broadcast message asking users to delete unneeded messages.
  - Look at user usage reports to determine which users are using a lot of space, and talk to them about it.
  - Delete unneeded mailboxes that might be filling up with broadcast messages.
  - Reduce the maximum space allowed for some or all mailboxes so the system tells users their mailboxes are full.
  - Reduce the read message retention time on some or all mailboxes so that the automatic message deletion cleans up more messages sooner.

- In an application using automatic read message deletion, disk usage typically increases from Monday to Friday. Disk usage decreases over the weekend as read messages are deleted and few new ones are created. When you understand these patterns you can better plan a strategy to deal with disk space problems.
- If the system is chronically low on space, consider purchasing additional storage from Nortel Networks, particularly if you must add new users to the system.

General methods to monitor disk space

Introduction

You have several ways to monitor how much disk space is available on your system.

Disk Usage window

In the Disk Usage window, available from the System window, you can view the current status of your hard disk to verify how much disk space is available.

Server Performance Monitor

The Server Performance Monitor (SPM) provides detailed information on the disk space available on the system.

Refer to Section A: “Monitoring the CallPilot server performance,” on page 459.

Reporter

In Reporter, you can view reports about system performance after you perform a download of OMs from the server to your administrative PC.

The Multimedia File System Usage report helps you determine if the level of user messages is getting too high. The Disk Usage Report provides information on the usage of all disk drives on the server.

For more information, refer to the *CallPilot Reporter Guide* (NTP 555-7101-310).

Administrative actions

You can perform certain actions to reduce the amount of used disk space.

Message retention

Decrease the amount of time that the system retains messages before they expire if you discover that the MMFS is getting full.

Storage space

Reduce the amount of storage space that is allocated to users. You can change this requirement only after the fact (for example, in case a user already has many messages stored in his or her mailbox).

OM retention

The system database collects OMs on the hard disk depending on the type of specified OMs and for a specified amount of time. If the database is getting full, reduce the amount of time for which those OMs are collected and retained on the hard disk.

ATTENTION

Because the hard disk is partitioned, reducing the message retention time affects only the MMFS. Reducing the OM retention time affects only the database storage levels.

See also

For more information on message retention and storage space allocation, refer to the CallPilot Manager online Help topics “Changing resource usage controls for mailbox class members” and “Controlling resource usage by mailbox owners.”

For more information on OM retention

- See “Collecting report data” on page 463.
- Refer to the *CallPilot Reporter Guide* (NTP 555-7101-310).

Section D: Monitoring the database

In this section

Monitoring the database using alarms

Introduction

The database stores user information, system configuration information, and various statistics that are collected by the system. You cannot monitor the database disk space directly. However, an alarm is raised if the database reaches its expected limit.

Database limits

The database is created during installation. It is designed to be large enough to store the full amount of anticipated system data. Under normal operation, the database should never fill up.

In some systems, particularly new ones for which usage patterns have yet to be established, the database can approach its expected limit. If this happens, you must determine the cause and provide a solution.

ATTENTION

As a precaution against disk failure, the database expands slightly to accommodate data beyond the anticipated limit. However, this is a safety feature. The underlying problem must be addressed as soon as possible.

Causes and solutions

System and user information use only small amounts of database disk space and will not fill up the database. The following are likely reasons why the database reaches its anticipated limit:

OMs are too detailed or stored for too long

OMs are statistics collected by the system. Based on the level of detail and the length of time for which these statistics are stored in the database, more or less disk space is used.

To reduce the amount of OM data that is collected, you must reduce the retention period or change the level of detail for which the system collects statistics. Refer to

- the CallPilot Manager online Help topic “Collecting report data”
- Reporter online Help

Note: When you lower the retention period for OMs you do not affect the MMFS. Similarly, lowering the retention period for user messages has no impact on the database. You must be clear about which parts of the hard disk (either the database or the MMFS) are approaching a point where they are nearly full.

The system is under-engineered

Systems are shipped with a database large enough to accommodate the initial requirements of customers. If your estimated usage patterns change or if your number of users grow, you might need to purchase additional disk space. Contact your distributor for details.

Chapter 23

Viewing and filtering server events

In this chapter

About CallPilot server events

Introduction

This chapter describes how to view and filter events that are generated by the CallPilot server.

Events

Events are occurrences on the CallPilot server, such as applications opening or closing, or errors being reported. These events appear in

- Windows NT Event Viewer on the server
- CallPilot Manager Event Browser and Alarm Monitor

Note: The Alarm Monitor does not report information-level events.

Event severity

Events are categorized by severity, as described below.

Critical

These events indicate that a service-affecting condition has occurred and an immediate corrective action is required. Critical events are reported when a component is completely out of service and you must take immediate action to restore it. For example, an event can indicate that the file system has crashed.

Major

These events indicate that a service-affecting condition has developed and an urgent corrective action is required. The event condition can cause severe degradation in server performance, and you must restore full capacity. For example, the event can indicate that the file system is 100 percent full.

Minor

These events indicate that a non-service-affecting fault condition exists, and that you must take corrective action to prevent a more serious fault. For example, an event can indicate that the file system is 90 percent full.

Information

These events indicate that something noteworthy has happened on the system, but do not mean that there is a problem. For example, an information-level event can indicate that a service has started or stopped. These events are displayed in the Event Browser but not in the Alarm Monitor.

System events

System events, such as Windows NT driver events, appear as event code 40592 in the Event Browser and in the system log in the Windows NT Event Viewer.

Security events

Security auditing is enabled on the server. Suspicious actions by a user are logged as event code 40593 in the Event Browser and in the security log in the Windows NT Event Viewer. This is an information event, so it does not appear in the Alarm Monitor.

Using the Event Browser versus the Alarm Monitor

Introduction

The Event Browser and Alarm Monitor both show events that occur on the server. These programs provide many common features for viewing events. The table below lists each feature and the program that offers the feature.

The main advantage for the Event Browser is that you can perform detailed filtering by several categories, including severity and event code range. You can also specify a number of latest events to view, so that you see only recent events.

The main advantage for the Alarm Monitor is that it shows (and therefore focuses on) Minor, Major, and Critical events, and ignores Information events. This enables you to focus on problems that require correction. In addition, when an event occurs repeatedly, it is reported only one time in the Alarm Monitor to avoid cluttering the Alarm Monitor display. You can also define SNMP parameters through the Alarm Monitor.

Event Browser versus Alarm Monitor feature matrix

Feature	**in Event Browser**	**in Alarm Monitor**
view events	Yes	Yes
view online Help for an event	Yes	Yes
save a list of events	Yes	No
print a list of events	Yes	No

Feature	in Event Browser	in Alarm Monitor
view minor, major, critical events	Yes	Yes
view information events	Yes	No
filter events by code, type, severity, latest events	Yes	No
customize event properties (severity and throttling parameters)	Yes	No[a]
clear an event	No	Yes
define SNMP filtering criteria	No	Yes

[a] Events can be customized in the Event Browser. However, these changes also affect the generated alarms.

Changing the event log size

Introduction

The event log resides on the server and stores a record of all events that occur on the server. You must log on to the server to change the event log size.

CAUTION

Risk of affecting server performance

Only qualified Nortel Networks technicians should make changes to the log settings. If you change the size settings, the results affect the performance of the server and the number of events that can be stored.

Event log wraparound

The event log size is fixed. It does not increase in size as new events are added to the log. When the log is full and a new event is generated, the server removes the *oldest* event report in the log and replaces that record with the newest one.

CAUTION

Risk of affecting server performance

Do not change the event log wrapping mechanism and size.

Impact of log size changes

If you reduce the size of the event log, then the server can store fewer events. If you increase the event log size, you reduce the amount of available disk space on the server and might slow the response times for retrieving events from the Event Browser.

Application events such as CallPilot events are stored in the Application log. If you change the Application log size, you also change the number of CallPilot events that are stored.

Default event log size

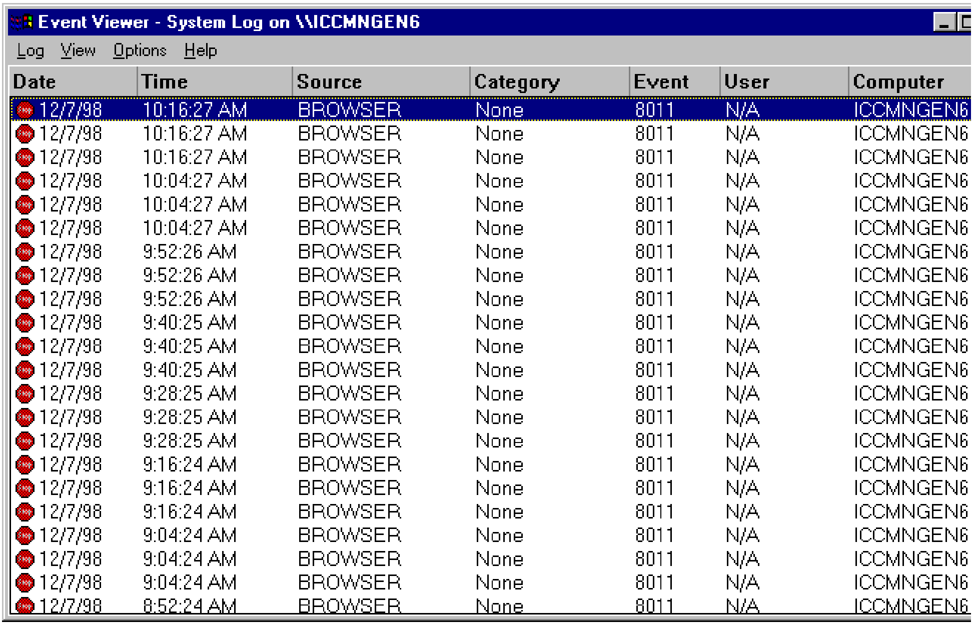
If you change the log size for the CallPilot server, do not use the Default button. The settings for this button correspond to the Windows NT default settings. During a CallPilot installation, the log settings are set to the following defaults:

Log name	Size	Event log wrapping
Application log	8 Mbytes	Overwrite events as needed.
System log	512 kbytes	Overwrite events as needed.
Security log	512 kbytes	Overwrite events as needed.

To change the event log size

1. Log on to the server as Administrator.
2. Click **Start** → **Programs** → **Administrative Tools (Common)** → **Event Viewer**.

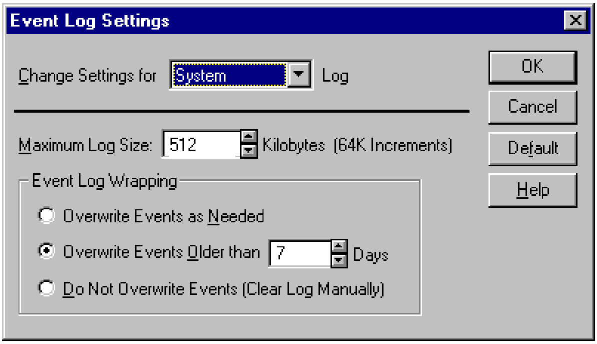
   Result: The Event Viewer appears.



Date	Time	Source	Category	Event	User	Computer
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	8:52:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6

3 Click **Log** → **Log Settings**.

Result: The Log Settings dialog box appears.



Event Log Settings

Change Settings for System Log

Maximum Log Size: 512 Kilobytes (64K Increments)

Event Log Wrapping

○ Overwrite Events as Needed

● Overwrite Events Older than 7 Days

○ Do Not Overwrite Events (Clear Log Manually)

4 Change the size of each log in the dialog box.

Note: CallPilot events are stored in the Application log. Change the Application log size to change the number of CallPilot events that are stored.

5 Click **OK** to accept the changes.

6 Click **File** →**Close**.

Using the Windows NT Event Viewer

Introduction

The Windows NT Event Viewer on the CallPilot server provides event and log information. Most information provided by the Event Viewer on the server can also be viewed through the Event Browser in CallPilot Manager.

When to use

Use the Windows NT Event Viewer on the server to view information that you cannot view through the Event Browser in CallPilot Manager. This information includes

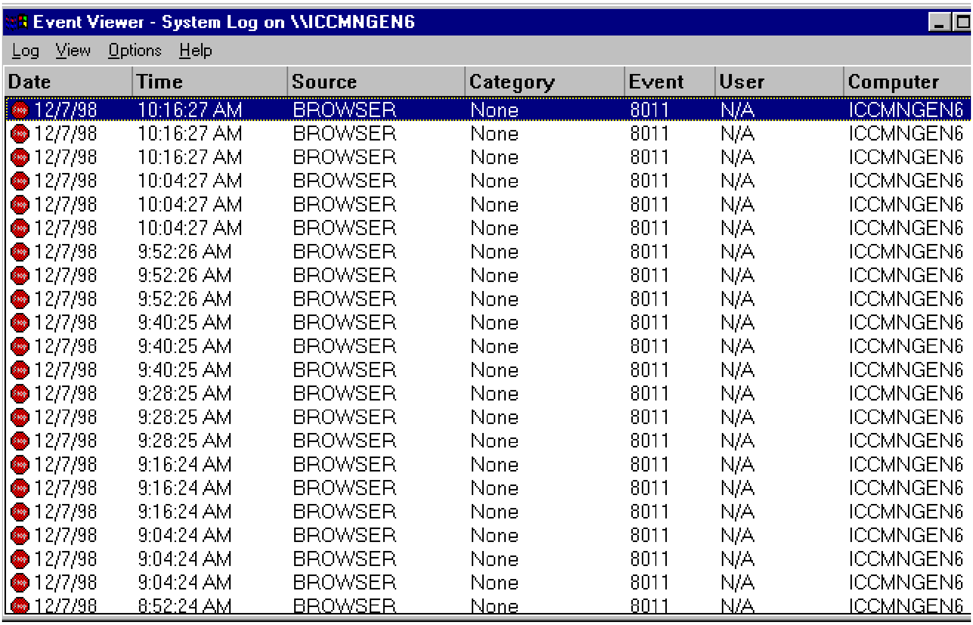
- database events (from the application log)
- server debug events (from the application log)

To open the Windows NT Event Viewer

1 Log on to the server as Administrator.

2 Click **Start** → **Programs** → **Administrative Tools (Common)** → **Event Viewer**.

Result: The Event Viewer appears.



Event Viewer - System Log on \\ICCMNGEN6

Date	Time	Source	Category	Event	User	Computer
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	8:52:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6

3 From the **Log** menu, select one of the following options:

- Click **Application** to view application, database, and server debug events. This log includes CallPilot application events.
- Click **Security** to view security events.
- Click **System** to view system events.

Section A: Using the Event Browser

In this section

Viewing events in the Event Browser

Introduction

The Event Browser shows events that occur on the server.

Default filtering

By default, only the latest 100 critical events are displayed in the Event Browser. You can change the filter to view all events. For more information, see “Filtering events in the Event Browser” on page 497.

To access the Event Browser

In CallPilot Manager, click System → Event Browser to view the Event Browser page.

To view help for event codes

The online Help contains more information about each entry, including a recovery path to correct or further investigate the problem. To view additional details on an event, click the event code.

Filtering events in the Event Browser

Introduction

To reduce the number of events shown in the Event Browser at one time, you can define filter settings to display only those events that match your criteria.

The default filter setting shows the latest 100 critical events.

Filter options

The filter combines the filter settings from each category.

You can set the filter to display

- a specific number of latest events or all events that are retrieved from the server
- events of a certain severity (critical, major, minor, information)
- a specific event code range, or all event codes
- a specific type of alarm (alarm set, alarm cleared, or message)
- events that occurred during a specific date and time interval

Example

At BestAir (an imaginary company name used in examples only), system engineer Jane Oliver is testing a new server component. Before she performs the tests, she changes the filtering criteria to display all events, including information events. These events tell her whether system components are starting up or not. When Jane finishes her tests, she changes the filtering criteria back to the default setting.

Looking up procedures in the CallPilot Manager online Help

To find procedures in the online Help, look up **Event Browser** and **events** in the online Help index.

Saving and printing a list of events from the Event Browser

Introduction

You can save or print the events listed in the Event Browser. All events listed in the Event Browser are saved or printed. If you have a problem with your system the log can help technical support representatives conduct a thorough analysis of your system.

Looking up procedures in the CallPilot Manager online Help

To find procedures in the online Help, look up **Event Browser** and **events** in the online Help index.

Section B: Using the Alarm Monitor

In this section

Viewing alarms in the Alarm Monitor

Introduction

The Alarm Monitor displays a list of CallPilot server alarms.

Alarms are warnings generated by events. Alarms communicate the same information as events. However, alarms are reported in the Alarm Monitor instead of the Event Browser, and are managed differently than events:

- Alarms appear in the Alarm Monitor only for Minor, Major, and Critical events (not Information events). All events can be reported in the Event Browser (depending on filtering criteria defined in the Event Browser)
- The first time an event occurs, it generates an alarm that appears in the Alarm Monitor. If the same event continues to occur, a new alarm is not generated. Instead, the time and date assigned to the original generated alarm is updated.
- If you filter events in the Event Browser, this does not affect the Alarm Monitor. The Alarm Monitor displays all Minor, Major, and Critical alarms in the Alarm Monitor.
- If you customize events in the Event Browser, those changes do affect the Alarm Monitor. For example, if an event's severity is changed from Minor to Information, the event does not generate an alarm. Also, if an event's severity is changed from Minor to Major, the severity of the generated alarm will be Major.
- Alarms can be cleared from the Alarm Monitor, but the event that generated the alarm is not cleared from the event log or the Event Browser.

To access the Alarm Monitor

In CallPilot Manager, select System → Alarm Monitor to view the Alarm Monitor page.

To view help for event codes

The Alarm Monitor lists details about the alarms, including the event code that generated the alarm.

The online Help contains more information about events, including a recovery path to correct or further investigate the problem. To view additional details on an event, click the event code.

Filtering SNMP traps

Introduction

You can access the SNMP Settings page from the Alarm Monitor to determine which SNMP traps, based on severity, are sent out from CallPilot. For more information on SNMP, see Section D: “Configuring CallPilot to send SNMP traps to a Network Management System,” on page 513.

Looking up procedures in the CallPilot Manager online Help

To find the online Help procedure, look up **SNMP** in the online Help index.

Clearing active alarms

When to use

You can clear alarms from the Alarm Monitor in one of two ways:

- The CallPilot server automatically clears alarms when the alarm condition changes.
- You can clear alarms manually.

When you clear an alarm you remove the selected alarm (but not the event that raised it) from the list shown in the Alarm Monitor. The event that generated the alarm can still be viewed in the Event Browser. If the event occurs again, however, the alarm reappears in the Alarm Monitor.

Example

At BestAir, an alarm appears with the description “Disk is 90% full.” Mark Brown, the system administrator, checks the system disk space, removes temporary files, and considers ordering a larger hard drive. Only after he has resolved the problem does he clear the alarm from the Alarm Monitor.

Getting there

CallPilot Manager → System → Alarm Monitor

Looking up procedures in the CallPilot Manager online Help

To find the online Help procedure for clearing an alarm, look up **alarms** in the online Help index.

Section C: Throttling and customizing events

In this section

Throttling events (reducing the frequency of events)

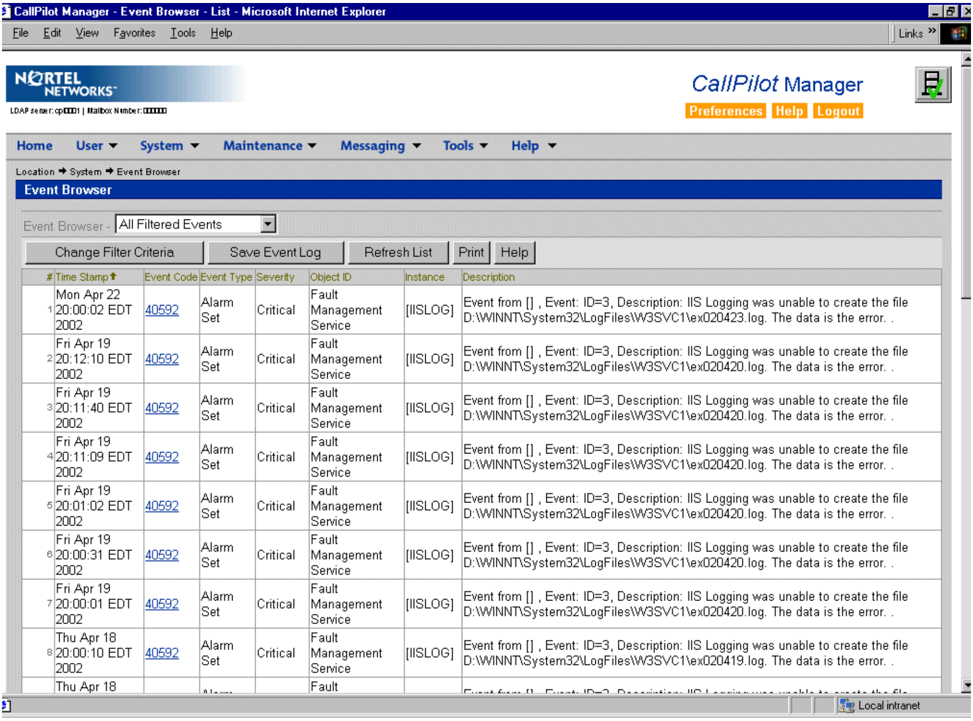
Introduction

Event throttling lets you control the frequency with which the same event is recorded by the event log and appears in the Event Browser, Alarm Monitor, and Windows NT Event Viewer. This prevents these windows and the event log from becoming overcrowded. If too many instances of each event are recorded, there might not be enough space in the event log to record more important events. Also, viewing too many instances of each event can overwhelm users, causing them to overlook important events.

To set throttling on only specific event codes

To set throttling on specific event codes, see the CallPilot Manager online Help topic “Throttling events (reducing the frequency of events).”

Getting there CallPilot Manager → System → Event Browser


CallPilot Manager - Event Browser - List - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
NORTEL NETWORKS
LDAP server: cp[illegible] | Mailbox Number: [illegible]
CallPilot Manager
Preferences
Help
Logout
Home
User
System
Maintenance
Messaging
Tools
Help
Location → System → Event Browser
Event Browser
Event Browser - All Filtered Events
Change Filter Criteria
Save Event Log
Refresh List
Print
Help
Local intranet

#	Time Stamp	Event Code	Event Type	Severity	Object ID	Instance	Description
1	Mon Apr 22 20:00:02 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020423.log. The data is the error. .
2	Fri Apr 19 20:12:10 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
3	Fri Apr 19 20:11:40 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
4	Fri Apr 19 20:11:09 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
5	Fri Apr 19 20:01:02 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
6	Fri Apr 19 20:00:31 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
7	Fri Apr 19 20:00:01 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
8	Thu Apr 18 20:00:10 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020419.log. The data is the error. .
	Thu Apr 18		Alarm		Fault		Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file

Looking up procedures in the CallPilot Manager online Help

To find the online Help procedure for throttling events, look up **events** in the online Help index.

Filtering by changing event properties

Introduction

You might want to override the default severity or throttling parameters of any event code for the following reasons:

- to increase the severity of an event (for example, from information to minor) so that the event is displayed in the Alarm Monitor when it occurs
- to reduce the severity of a recurring alarm to *information* so that the event does not appear in the Alarm Monitor
- to set the throttling parameters to reduce the frequency an event is generated

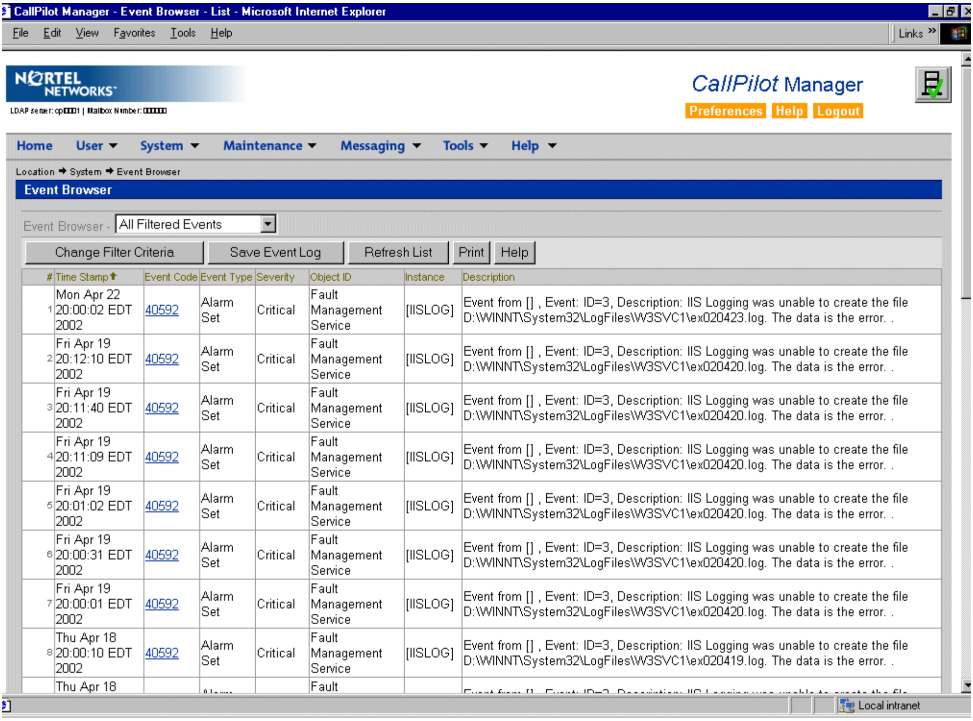
Previous occurrences of the event are not affected. You can revert to the default event definition at any time by deleting the customized version of the event.

Example

At BestAir, CallPilot server is generating a critical alarm because of a database error. The system engineer, Jane Oliver, has ordered a replacement for the malfunctioning disk drive that is causing the problem. Since she is aware of the problem, Jane does not want to see an alarm in the Alarm Monitor every time the error occurs.

Jane can customize this event to reduce the severity of the error from critical to information. After the new disk is installed, she can delete the event preference to restore the severity to critical.

Getting there CallPilot Manager → System → Event Browser


CallPilot Manager - Event Browser - List - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links »
NORTEL NETWORKS
CallPilot Manager
Preferences Help Logout
Home User ▾ System ▾ Maintenance ▾ Messaging ▾ Tools ▾ Help ▾
Local intranet

LDAP server: cp[redacted]1 | Mailbox Number: [redacted]

Location ➔ System ➔ Event Browser

Event Browser

Event Browser - All Filtered Events

Change Filter Criteria | Save Event Log | Refresh List | Print | Help

#	Time Stamp ⬆	Event Code	Event Type	Severity	Object ID	Instance	Description
1	Mon Apr 22 20:00:02 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020423.log. The data is the error. .
2	Fri Apr 19 20:12:10 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
3	Fri Apr 19 20:11:40 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
4	Fri Apr 19 20:11:09 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
5	Fri Apr 19 20:01:02 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
6	Fri Apr 19 20:00:31 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
7	Fri Apr 19 20:00:01 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020420.log. The data is the error. .
8	Thu Apr 18 20:00:10 EDT 2002	40592	Alarm Set	Critical	Fault Management Service	[IISLOG]	Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file D:\WINNT\System32\LogFiles\W3SVC1\ex020419.log. The data is the error. .
	Thu Apr 18		Alarm		Fault		Event from [] , Event: ID=3, Description: IIS Logging was unable to create the file

Looking up procedures in the CallPilot Manager online Help

To find the online Help procedure for throttling events, look up **events** in the online Help index.

Section D: Configuring CallPilot to send SNMP traps to a Network Management System

In this section

Overview

Introduction

This section describes how to configure the CallPilot server to send Simple Network Management Protocol (SNMP) traps to a Network Management System (NMS). When this service is configured you can work with server alarms on an NMS.

Two examples of NMS clients that you can configure to use this service are the OTM Alarm Notification and the HP Openview tools. The procedure in this section uses the OTM Alarm Notification tool as one example of how to configure an NMS.

The configuration has two parts:

- configuring SNMP on the CallPilot server so that the traps are directed to an NMS
- configuring the NMS so that it can receive the CallPilot SNMP traps

Configuring SNMPs on the CallPilot server

Introduction

Windows NT provides a Simple Network Management Protocol (SNMP) v2 agent that runs as a service on the CallPilot server. This service can be configured so that the SNMP traps generated by the CallPilot server are directed to a Network Management System (NMS) that resides on your site network.

In the following procedure, you stop the SNMP service, configure SNMP, and then restart the SNMP service.

To configure SNMP to forward traps to an NMS

1 On the CallPilot server, select **Start** → **Settings** → **Control Panel**. Double-click Services.

Result: The Services window appears.

2 In the **Services** list, select **SNMP**.

3 Click **Stop**.

Result: The SNMP service stops.

4 Click **Close**.

Result: The Services window closes.

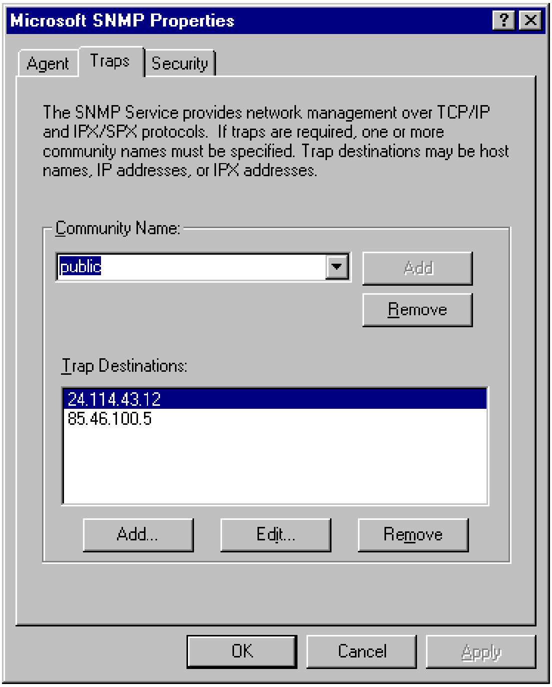
5 From the **Control Panel**, double-click **Network**.

Result: The Network window appears.

6 Select the **Services** tab.

7 In the list of Network Services, select **SNMP Service**. Click **Properties**.

Result: The Microsoft SNMP Properties window appears.



Microsoft SNMP Properties

The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses, or IPX addresses.

Community Name: public

Trap Destinations:

24.114.43.12
85.46.100.5

8 Select the **Traps** tab.

9 If no community name is defined in the **Community Name** field, type **public**. Click **Add**.

10 To add a trap IP destination, go to the bottom of the **Trap Destinations** list box and click **Add**.

Result: The Service Configuration window appears.

11 Type in the trap IP address of the NMS you want to use. Click **Add**.

Result: The IP address is added.

12 Repeat steps 10 and 11 to add all the NMS clients that you want to receive the traps.

13 Click **OK**.

Result: The Microsoft SNMP Properties window closes.

14 Click **Close**.

Result: The Network window closes.

15 From the **Control Panel**, double-click **Services**.

Result: The Services window appears.

16 In the **Services** list, select **SNMP**.

17 Click **Start**.

Result: The SNMP service starts.

18 Click **Close**.

Result: The Services window closes.

Configuring an NMS to receive CallPilot traps

Introduction

Once the CallPilot server is configured to send traps to an NMS, then you configure the Network Management System (NMS) to receive these traps.

The following procedure uses the OTM Alarm Notification tool as an example of how to configure an NMS.

Network Management Systems

There are a number of NMS systems that you can use to receive and interpret traps. Each one requires a different setup.

This chapter covers the OTM Alarm Notification NMS only. However, by using the CallPilot Management Information Base (MIB) files it should be possible to set up other NMS systems to interpret CallPilot traps.

Management Information Base files

The CallPilot SNMP MIB files describe the CallPilot trap format. The network administrator might want to look at these files when configuring an NMS to receive CallPilot SNMP traps.

The MIB files are nbflt.mib and nt-ref.mib. They are SNMP v2 MIB files and can be used on an NMS system.

The MIB files are available

- on the CallPilot Server CD, in the directory platform\default\nortel\data\
- on the CallPilot server in the directory D:\Nortel\data\

Alarms

The CallPilot server generates alarms. Alarms with the following severity levels are sent out as SNMP traps to the NMS:

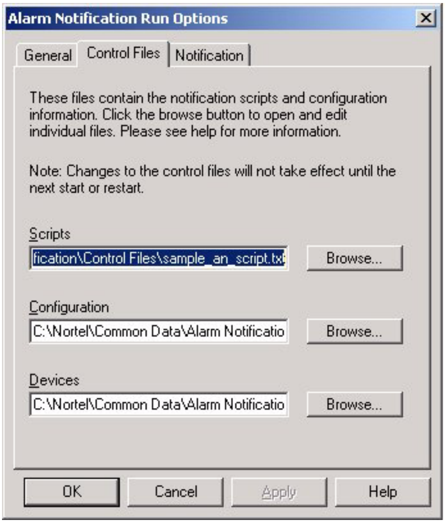
- 0 undefined
- 1 critical
- 2 major
- 3 minor

To configure OTM Alarm Notification to receive CallPilot SNMP traps

1 From the **OTM Alarm Notification** window, select **Configuration → Run Options**.

Result: The Alarm Notification Run Options Property Sheet appears.

2 Select the **Control Files** tab. The Control Files tab lists three files: Devices.txt, Config.txt, and Scripts.txt. You must modify each of these files.



These files contain the notification scripts and configuration information. Click the browse button to open and edit individual files. Please see help for more information.

Note: Changes to the control files will not take effect until the next start or restart.

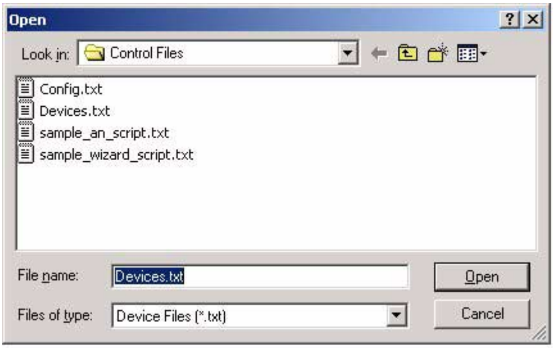
Scripts: fication\Control Files\sample_an_script.txt

Configuration: C:\Nortel\Common Data\Alarm Notificatio

Devices: C:\Nortel\Common Data\Alarm Notificatio

3 To modify Devices.txt, click Browse beside the file name.

Result: The Open dialog box appears with the file name selected.



Note: The above dialog box example shows the default files that are provided when OTM is installed. The remainder of this procedure refers to the default file names.

4 Click Open.

Result: The file opens in an editor where you can modify the file.

5 In the Devices.txt file, add the following line:

```
CALL_PILOT IP_ADDRESS_OF_SERVER
```

where:

`CALL_PILOT` is the name displayed under Device Type in the OTM Alarm Notification window. It can be any value.

`IP_ADDRESS_OF_SERVER` is the actual IP address of the server that sends the traps to this NMS client.

Example: CALL_PILOT 47.235.12.85

6 To modify Config.txt, click Browse beside the file name.

Result: The Open dialog box appears with the file name selected.

7 Click Open.

Result: The file opens in an editor where you can modify the file.

8 In the Config.txt file, add the following block of text:

```
...
```

```
device CALL_PILOT 6.1 6.2 6.3 6.4 {

   1.3.6.1.4.1.562.3.8.2.5.2.1.2.0 string
$nbFltAlarmTimeStamp "Event Time"

   1.3.6.1.4.1.562.3.8.2.5.2.1.3.0 integer
$nbFltAlarmEventCode "Error Code"

   1.3.6.1.4.1.562.3.8.2.5.2.1.4.0 integer
$nbFltAlarmEventType "Alarm Type"

   1.3.6.1.4.1.562.3.8.2.5.2.1.5.0 integer
$nbFltAlarmEventSeverity "Severity"

   1.3.6.1.4.1.562.3.8.2.5.2.1.8.0 string
$nbFltAlarmOriginator "Component Name"

   1.3.6.1.4.1.562.3.8.2.5.2.1.9.0 string
$nbFltAlarmDescription "Operator Data"

}
```

...

where:

CALL_PILOT is the same name that is defined in the Devices.txt file.

9 To modify sample_an_script.txt, click Browse beside the file name.

Result: The Open dialog box appears with the file name selected.

10 Click Open.

Result: The file opens in an editor where you can modify the file.

11 In the sample_an_script.txt file, add the following blocks of text:

...

/* This is a sample definition for using a log file. All events sent to this notification are appended to the filename defined below. Note that Windows “long” file names are not supported. */

```
notification file CALLPILOT_file {

   filename:="c:\Nortel\callpilot_log.txt";

}
```

```
...
/* This is a sample definition for using a numeric pager */
notification npager CALLPILOT_NumericPager {
phone:="9,378-6388";
...
/* if pager has PIN number insert */
/* pin:="101565"; */
}
...
```

where:

`CALLPILOT_NumericPager` is any name (it is used in the script code below)

"`9,378-6388`" is the pager number

...

```
/******************************/
/* Scripts for CALLPILOT Traps */
/******************************/
/* Add the following lines */
script CALLPILOTScript {
/* This rule looks for all CallPilot events and remaps them to the
OTM event format */
   rule check_critical {
      if ($CurrentTrapDevice="CALL_PILOT") {
    /* Prints event to OTM Alarm Notification console - optional*/
         send(con,"CALLPILOT alarm: ",
$nbFltAlarmTimeStamp," - " ,
$nbFltAlarmEventCode," - " ,
$nbFltAlarmEventType," - " ,
$nbFltAlarmEventSeverity," - ",
$nbFltAlarmOriginator," - ",
$nbFltAlarmDescription);
        /* Appends event to log file - optional*/
         send(CALLPILOT_file,"NGEN alarm: ",
$nbFltAlarmTimeStamp," - " ,
$nbFltAlarmEventCode," - " ,
$nbFltAlarmEventType," - " ,
$nbFltAlarmEventSeverity," - ",
$nbFltAlarmOriginator," - ",
$nbFltAlarmDescription);
        /* Sends message to numeric pager - optional */
send(NGEN_NumericPager,$nbFltAlarmEventCode);


         }
   }
}
...
```

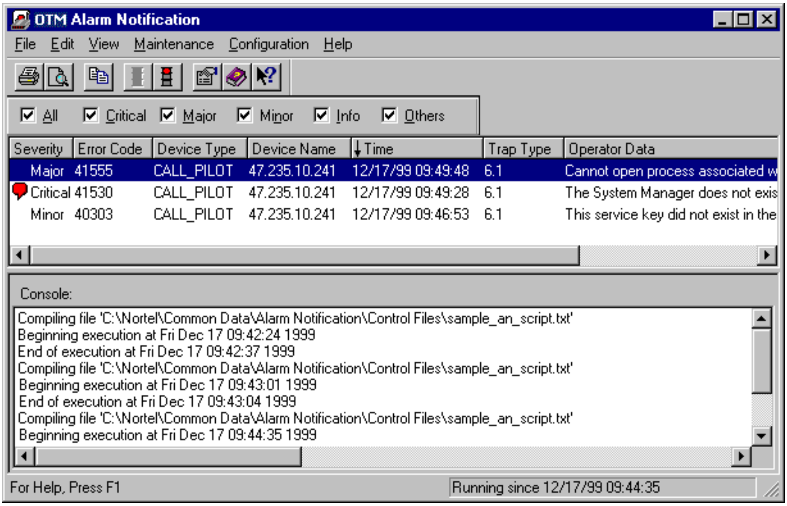
Note: By default, these three files are located in C:\Nortel\Common Data\Alarm Notification\Control Files, but this is user selectable on installation of OTM.

12 After modifying the files, click **OK**.

Result: The Alarm Notification Run Options Property Sheet closes.

13 In the **OTM Alarm Notification** window, select **Maintenance** → **Start**.

Result: CallPilot traps appear in the OTM Alarm Notification window list view as they are generated by the CallPilot server.


OTM Alarm Notification
File Edit View Maintenance Configuration Help
☑ All ☑ Critical ☑ Major ☑ Minor ☑ Info ☑ Others

Severity	Error Code	Device Type	Device Name	Time	Trap Type	Operator Data
Major	41555	CALL_PILOT	47.235.10.241	12/17/99 09:49:48	6.1	Cannot open process associated w
Critical	41530	CALL_PILOT	47.235.10.241	12/17/99 09:49:28	6.1	The System Manager does not exis
Minor	40303	CALL_PILOT	47.235.10.241	12/17/99 09:46:53	6.1	This service key did not exist in the

Console:

```
Compiling file 'C:\Nortel\Common Data\Alarm Notification\Control Files\sample_an_script.txt'
Beginning execution at Fri Dec 17 09:42:24 1999
End of execution at Fri Dec 17 09:42:37 1999
Compiling file 'C:\Nortel\Common Data\Alarm Notification\Control Files\sample_an_script.txt'
Beginning execution at Fri Dec 17 09:43:01 1999
End of execution at Fri Dec 17 09:43:04 1999
Compiling file 'C:\Nortel\Common Data\Alarm Notification\Control Files\sample_an_script.txt'
Beginning execution at Fri Dec 17 09:44:35 1999
```

For Help, Press F1 Running since 12/17/99 09:44:35

Part 7

Troubleshooting

In this part

Chapter 24

Troubleshooting a CallPilot server

In this chapter

Overview

Introduction

CallPilot Manager provides the following tools to help you monitor and troubleshoot the CallPilot server.

- Use the Event Browser to interpret error messages and find information to troubleshoot the CallPilot server.
- Use the Alarm Monitor stay informed of server operation problems.
- Use the Maintenance page to run diagnostic tests on the server.
- Use Reporter to isolate information about the server and document changes that result from troubleshooting activities.
- Refer to the CallPilot Desktop Messaging Administration and Maintenance Guide for troubleshooting information for administrators of desktop messaging and My CallPilot users.

You can also check the following sources to help you identify the source of a problem:

- the Event log on the computer running CallPilot Manager.
- the Event log on the CallPilot server.
- error messages displayed on the computer running CallPilot Manager
- Internet Services Manager
- Windows Services interface
- release information for your web browser, web server, and CallPilot

See also

Refer to specific online Help Troubleshooting topics for solutions to specific problems (such as mailbox configuration problems) that may occur.

Troubleshooting backup and restore operations

Introduction

Whenever you back up or restore CallPilot information, monitor the operation and, if there are errors, view the log file that was generated for the operation.

- The backup log files are located in D:\nortel\data\backup\BackupLogs
- The restore log files are located in D:\nortel\data\backup\RestoreLogs

See also

See Chapter 8, “Backing up and restoring CallPilot information.”

Refer to the CallPilot Manager online Help book “Troubleshooting backup and restore operations.”

Troubleshooting Symposium Voice Services support

Introduction

If you need to troubleshoot Symposium Voice Services support, the following might happen:

- The Event Browser will display a Meridian Link TSP or ACCESS link event.
- Mailbox owners will notice that calls are not answered.

Meridian Link TSP events

System event codes in between 43000 and 43299 identify Meridian Link TSP events.

These include

- 43000 (Meridian Link is not operating)
- 43002 (Meridian Link is operating)
- 43004 (The TSP has started)

ACCESS link events

Application event codes between 60900 and 60999 identify ACCESS link events.

These include:

- 60920 (ACCESS link is not operating)
- 60921 (ACCESS link is operating)

Problem diagnosis configuration checklist

- Is voice port configuration consistent across all subsystems?
- On the CallPilot server:
  - Is the Symposium Call Center server (SCCS) IP address properly configured?
  - Is the CDN for ACCESS channels configured as the Symposium Voice Services SDN?
  - Is the CDN for IVR channels configured as the Symposium Voice Services support announcement or voice menu SDN?
  - Does the Class ID configured via Configuration Wizard equal the ACCESS port channel configured on the Symposium Call Center server?
- On the Symposium Call Center server:
  - Is the CallPilot ELAN IP address properly configured?
  - Does the ACCESS voice port channel equal the Class ID on the CallPilot server?
  - Is the port number configured as 10008?
- On the switch:
  - Is the CDN for ACCESS channels configured so that IVR=YES and ALOG=YES?
  - Is the CDN for IVR channels configured so that IVR=YES and ALOG=YES?
  - Are the ACCESS and IVR channels configured so that AST=0, 1 and CLS=MMA, FLXA?
  - Are all CallPilot server ELAN VAS IDs configured so that SECU=YES?

See also

- See Section D: “Configuring Symposium Voice Services support,” on page 415.
- For information on specific event codes, refer to the CallPilot Manager Event Browser.

- For help with troubleshooting, see the CallPilot Manager online Help Troubleshooting topic “Calls are not answered.”

Chapter 25

Preventing unnecessary maintenance

In this chapter

CallPilot preventive maintenance guidelines

1 **Maintain a Log Book.**

Maintain a logbook with the system where any maintenance activity performed should be recorded diligently. This can be extremely useful in diagnosing problems. This logbook should contain a description of the activity, who performed it, and when it was performed. Items to include are activities such as:

- system operations on the CallPilot server or the PBX such as an installations, upgrades, or PEP installations
- hardware replacement
- administrative updates such as
    - user additions, deletions, or modifications
    - system parameter changes
- problem investigation

2 **Allow only Qualified Technicians.**

It is important that only CallPilot qualified technicians are allowed to administer or maintain the CallPilot server. All activities performed on the CallPilot should have a name associated with the activity recorded in the logbook as mentioned in item 1 above.

3 Back up information regularly.

A regular backup schedule of the CallPilot server is probably the most important risk mitigation measure you can perform. CallPilot provides several backup options such as backup to tape, and backup to remote hard disk.

Refer to

- Chapter 8, “Backing up and restoring CallPilot information”
- Product Bulletin 2001-037 “CallPilot Remote Disk Backup Update”

For CallPilot server’s equipped with RAID, the RAID split procedure may also be useful. Refer to the document “702t and 1001rp Installation and Configuration update – Splitting the RAID drives”.

4 Check the Backup Logs.

Regularly verify that the backup was successful by looking at the backup logs in the directory: d:\Nortel\data\backup.

5 View the Alarm Monitor regularly.

A trained and experienced CallPilot technician is the best person to monitor the alarms on a regular basis. The CallPilot server is constantly generating alarms and events, which indicates normal operation. However, any unusual alarms or events, changes in alarm patterns, or inordinate alarm volumes should be investigated.

Refer to Chapter 23, “Viewing and filtering server events.”

6 Use CallPilot Reporter.

Reporter is another excellent tool to understand the usage of CallPilot. It will be useful in understanding the heavy users, the heavy usage times and other patterns.

Refer to the *CallPilot Reporter Guide*.

7 Monitor RAID Events

For RAID systems, ensure that RAID monitoring tools are installed. For DAC960 RAID cards this is DacMonitor. For AR352, this is Global Array Manager. Verify through the RAID monitoring tools that no drives have been marked dead or out of synch by the RAID card.

Also, this can be monitored through the event logs. Any events raised by ’DAC’ or ’AR352’ should be investigated as possible RAID problems.

Refer to “CallPilot Documentation Addendum”, April 2001 or the General Release Bulletin GR-134, Appendix-H.

8 Monitor MMFS volumes.

Verify using CallPilot Reporter that the MMFS usage is below 90% on all MMFS volumes. If any volume is above 90% then the mailboxes may have to be rebalanced to other volumes.

Refer to

- “Monitoring Multimedia File System volumes” on page 473
- *CallPilot Reporter Guide*.

9 Remove unused or “dead” mailboxes.

Use CallPilot Reporter to search for mailboxes that are no longer in use. Mailboxes that exist in the system but are not in use can take up valuable MMFS space as broadcast messages build up. Also, mailboxes that belong to former employees that are on the CallPilot system can cause a potential security concern.

Refer to the *CallPilot Reporter Guide*.

10 Monitor DS30 and DSP ports.

Regularly monitor DS30 and DSP ports using CallPilot Manager to make sure that none of the ports are Off Duty.

“Monitoring multimedia channels” on page 468.

11 Use Hacker Monitor sparingly.

Use Hacker Monitor only for necessary monitoring. Hacker monitor can fill up the Event Log and make it difficult to diagnose problems.

Refer to Chapter 9, “Monitoring suspicious activities.”

Index

CallPilot

Administrator’s 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 CallPilot server and the Meridian 1 switch or Succession CSE 1000 system 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:	555-7101-301
Product release:	2.02
Document release:	Standard 1.0
Date:	May 2003

NORTEL NETWORKS™