Administrator's Guide

CallPilot
Release 4.0

Document Number: 555-7101-301

Document Version: Standard 1.18

April 2007

NORTEL

Copyright © 2007 Nortel Networks.

All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

The process of transmitting data and call messaging between the CallPilot server and the switch or 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.

Trademarks

*Nortel Networks, the Nortel Networks logo, the Globemark, and Unified Networks, BNR, CallPilot, DMS, DMS-100, DMS-250, DMS-MTX, DMS-SCP, DPN, Dualmode, Helmsman, IVR, MAP, Meridian, Meridian 1, Meridian Link, Meridian Mail, Norstar, SL-1, SL-100, Succession, Supernode, Symposium, Telesis, and Unity are trademarks of Nortel Networks.

3COM is a trademark of 3Com Corporation.

ADOBE is a trademark of Adobe Systems Incorporated.

ATLAS is a trademark of Quantum Corporation.

BLACKBERRY is a trademark of Research in Motion Limited.

CRYSTAL REPORTS is a trademark of Seagate Software Inc.

EUDORA is a trademark of Qualcomm.

eTrust and InoculateIT are trademarks of Computer Associates Think Inc.

DIRECTX, EXCHANGE.NET, FRONTPAGE, INTERNET EXPLORER, LINKEXCHANGE, MICROSOFT, MICROSOFT EXCHANGE SERVER, MS-DOS, NETMEETING, OUTLOOK, POWERPOINT, VISUAL STUDIO, WINDOWS, WINDOWS MEDIA, and WINDOWS NT are trademarks of Microsoft Corporation.

GROUPWISE and NOVELL are trademarks of Novell Inc.

LOGITECH is a trademark of Logitech, Inc.

MCAFEE and NETSHIELD are trademarks of McAfee Associates, Inc.

MYLEX is a trademark of Mylex Corporation.

NETSCAPE COMMUNICATOR is a trademark of Netscape Communications Corporation.

NOTES is a trademark of Lotus Development Corporation.

NORTON ANTIVIRUS and PCANYWHERE are trademarks of Symantec Corporation.

QUICKTIME is a trademark of Apple Computer, In.

RADISYS is a trademark of Radisys Corporation.

SLR4, SLR5, and TANDBERG are trademarks of Tandberg Data ASA.

SYBASE is a trademark of Sybase, Inc.

TEAC is a trademark of TEAC Corporation

US ROBOTICS, the US ROBOTICS logo, and SPORTSTER are trademarks of US Robotics.

WINZIP is a trademark of Nico Mark Computing, Inc.

XEON is a trademark of Intel, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Publication history

April 2007	CallPilot 4.0, Standard 1.18 of the *Administrator's Guide* is issued for general release.
April 2007	CallPilot 4.0, Standard 1.17 of the *Administrator's Guide* is issued for general release.
October 2006	CallPilot 4.0, Standard 1.16 of the *Administrator's Guide* is issued for general release.
October 2006	CallPilot 4.0, Standard 1.15 of the *Administrator's Guide* is issued for general release.
September 2006	CallPilot 4.0, Standard 1.14 of the *Administrator's Guide* is issued for general release.
July 2006	CallPilot 4.0, Standard 1.12 of the *Administrator's Guide* is issued for general release.
April 2006	CallPilot 4.0, Standard 1.11 of the *Administrator's Guide* is issued for general release.
December 2005	CallPilot 4.0, Standard 1.10 of the *Administrator's Guide* is issued for general release.
November 2005	CallPilot 4.0, Standard 1.09 of the *Administrator's Guide* is issued for general release.
September 2005	CallPilot 4.0, Standard 1.08 of the *Administrator's Guide* is issued for general release.
August 2005	CallPilot 4.0, Standard 1.07 of the *Administrator's Guide* is issued for general release.
July 2005	CallPilot 4.0, Standard 1.06 of the *Administrator's Guide* is issued for general release.

July 2005	CallPilot 4.0, Standard 1.05 of the *Administrator's Guide* is issued for general release.
July 2005	CallPilot 4.0, Standard 1.04 of the *Administrator's Guide* is issued for general release.
July 2005	CallPilot 4.0, Standard 1.03 of the *Administrator's Guide* is issued for general release.
July 2005	CallPilot 4.0, Standard 1.02 of the *Administrator's Guide* is issued for general release.
July 2005	CallPilot 4.0, Standard 1.01 of the *Administrator's Guide* is issued for general release.
July 2005	CallPilot 4.0, Standard 1.0 of the *Administrator's Guide* is issued for general release.
November 2004	Standard 1.0 for CallPilot 3.0.
April 2004	Standard 2.0 for CallPilot 2.5.
October 2003	Standard 1.0 for CallPilot 2.5.
May 2003	Standard 1.0 issue for CallPilot 2.02 (2.01.27.05). 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

Chapter 1

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Chapter 2

CallPilot administration overview

In this chapter

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.

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

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 (PC). You log on to the server using a URL, with a user ID (mailbox number) and a password.

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

- Internet Explorer 6.0
- Netscape 6.2, 7.0, 7.1, and 7.2

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

ATTENTION

Netscape must not be installed on the CallPilot server.

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 information about using pcAnywhere from Symantec Corporation for setting up remote administration at an administrator's site.

One licensed copy of pcAnywhere 11.0 is provided for the server on the CallPilot server software CD. pcAnywhere 11.0 is also installed on the server at the factory.

ATTENTION

To install pcAnywhere 11.0 on the remote PC, you must purchase a separate license for the remote PC.

Logging on to the CallPilot server with CallPilot Manager

You must use a web browser to log on to and administer the CallPilot 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 host name or IP address, as well as the CallPilot server host name or IP address.

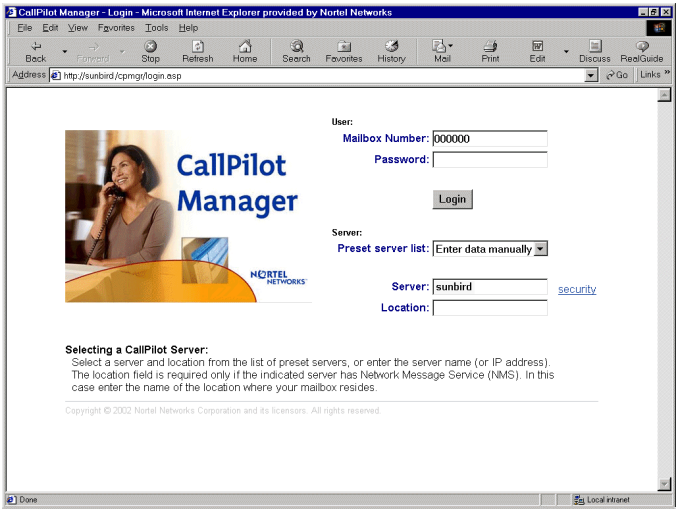
To log on to CallPilot Manager

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

2 Type the CallPilot Manager web server 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 screen appears.



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 23.
- Type the CallPilot server host name or IP address in the Server box.
- If you are using Microsoft Internet Explorer: To reuse information you entered during a prior session on the same PC, do the following:

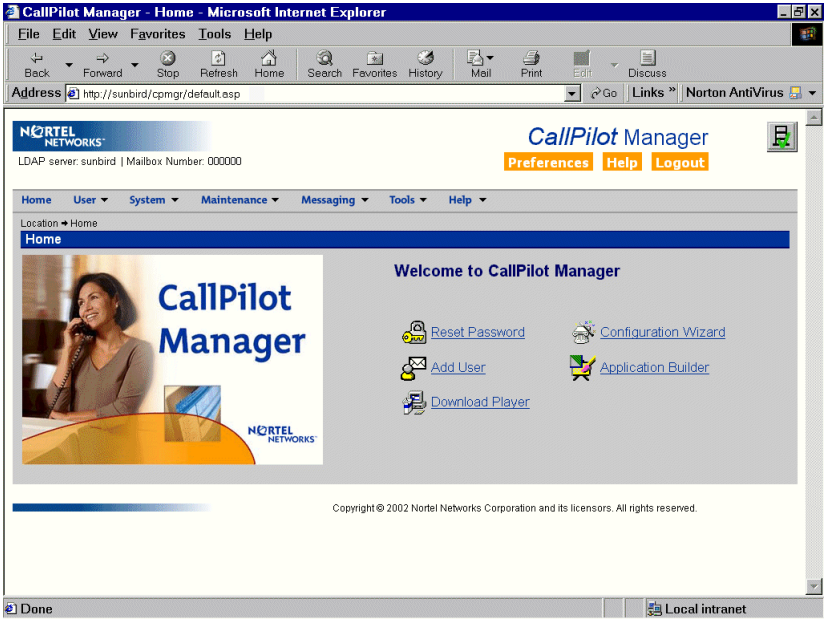
  a. Clear the contents in the box.

  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 screen appears.



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. Shortcuts that appear depend on the CallPilot Manager functions that you are permitted to use. For example, shortcuts to Reset Password and Add User appear only if you have user administration rights.

Determining the CallPilot server status

System ready indicator

The system ready indicator (SRI) 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

If you 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 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**

Setting security options for CallPilot Manager sessions

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 a pre-defined or manually specified server.

Getting there: **Preferences → Preferences page**

Delegation of administrative tasks

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 online Help and documentation

CallPilot online Help and documentation incorporate the following:

- CallPilot Manager online Help is the primary source of procedural information.
- The *CallPilot Administrator's Guide* (555-7101-301) provides an end-to-end overview of a CallPilot system. The CallPilot Administrator's Guide is available only in PDF format.

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 the server before proceeding. For installation instructions, refer to the *Installation and Configuration Task List* (555-7101-210) and the Server Installation Guide for your server.

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 Partner Information Center (PIC) at http://www.nortel.com/pic

  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. The process to issue a password can take up to 72 hours.

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

Troubleshooting

The *Troubleshooting Guide* (555-7101-501) describes symptoms that can appear on all CallPilot server platforms, and describes ways to resolve them. The *Troubleshooting Guide* (555-7101-501) is available from the Nortel PIC.

Using online sources

CallPilot administration online Help

The CallPilot Manager and CallPilot Reporter software contain online Help 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 screen to access the Administration Help area.
- Click the grey Help button on any screen to display a topic that relates to the contents of the screen.

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

The Application Builder software contains a Windows Help system.

CallPilot online Help for mailbox owners

My CallPilot software contains a Useful Information area that provides access to end-user guides. To access online Help for the currently selected My CallPilot tab, click the Help button on the upper right corner of the My CallPilot screen.

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 Nortel

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

http://www.nortel.com/documentation

Reference documents

- **Fundamentals**
  - CallPilot Fundamentals Guide (555-7101-010)
- **Planning and Engineering**
  - Planning and Engineering Guide (555-7101-101)
  - Network Planning Guide (555-7101-102)
  - Data Networking for Voice over IP Guide (553-3001-160)
- **Installation and Configuration**
  - Upgrade and Platform Migration Guide (555-7101-207)
  - Installation and Configuration Task List Guide (555-7101-210)
  - **Server Installation Guides**
    - 201i Server Hardware Installation Guide (555-7101-220)
    - 703t Server Hardware Installation Guide (555-7101-226)
    - 1002rp Server Hardware Installation Guide (555-7101-205)
    - 1005r Server Hardware Installation Guide (555-7101-228)
  - **Configuration and Testing Guides**
    - Meridian 1 and CallPilot Server Configuration Guide (555-7101-222)
    - T1/SMDI and CallPilot Server Configuration Guide (555-7101-224)
    - Succession 1000 System and CallPilot Server Configuration Guide (555-7101-510)
  - **Unified Messaging Software Installation**
    - Desktop Messaging and MyCallPilot Installation Guide (555-7101-505)
- **Administration**
  - Administrator's Guide (555-7101-301)
  - Software Administration and Maintenance Guide (555-7101-202)
  - Desktop Messaging and MyCallPilot Administration Guide (555-7101-503)
  - Meridian Mail to CallPilot Migration Guide (555-7101-801)
  - Application Builder Guide (555-7101-325)
  - Reporter Guide (555-7101-310)
- **Maintenance**
  - Troubleshooting Guide (555-7101-501)
  - **Server Maintenance and Diagnostics**
    - 201i Server Maintenance and Diagnostics Guide (555-7101-119)
    - 703t Server Maintenance and Diagnostics Guide (555-7101-227)
    - 1002rp Server Maintenance and Diagnostics Guide (555-7101-206)
    - 1005r Server Maintenance and Diagnostics Guide (555-7101-512)
    - Symposium, M1/Succession 1000, and Voice Processing Guide (297-2183-909)
- **End User Information**

End User Cards	End User Guides
Unified Messaging Quick Reference Card	Multimedia Messaging User Guide
Unified Messaging Wallet Card	Speech Activated Messaging User Guide
A-Style Command Comparison Card	Desktop Messaging User Guide for Microsoft Outlook
S-Style Command Comparison Card	Desktop Messaging User Guide for Lotus Notes
Menu Interface Quick Reference Card	Desktop Messaging User Guide for Novell Groupwise
Alternate Command Interface Quick Reference Card	Desktop Messaging User Guide for Internet Clients
	MyCallPilot User Guide

Chapter 3

Delegating administrative tasks

In this chapter

Overview

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.

If you are maintaining a staff of specialized administrators

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

Adding full administrators without mailboxes

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

Adding mailbox owners with some administrative privileges

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)
- shared distribution lists to which the administrator must be added (optional)
- 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

Adding an individual administrator

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**

Adding a group of administrators

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 Add**

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.

Getting there: **User → User Search → User Properties sheet**

Creating specialized administrators

If you are administering a CallPilot system with thousands of mailboxes, consider delegating 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. You need to know the tasks that are assigned to the mailbox owner, and the set of administrative rights required by the administrator.

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

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.

Examples of specialized administrators you can create

These examples 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 (RPL) administration rights (create special 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)
- RPL 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
- RPL 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 Email-by-Phone service. Classify these administrators as users with some administration rights with the following:

- Server settings administration rights
- Backup and 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
- RPL administration rights
- System prompt customization administration rights
- Application Builder administration rights (to set up voice menus and other custom applications)

Chapter 4

Mailbox administration

In this chapter

User creation templates and mailbox classes

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

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.

Using templates to create 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, 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.

Maintaining a set of user creation templates

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 Email-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

Creating and deleting user creation templates

Create user creation templates to facilitate adding large groups of mailbox owners with a single action.

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.

Customizing settings for new mailboxes

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 are unique for different mailboxes, leave them blank in the template.

Choosing a template for customization or duplication

When you choose a supplied template for customization or duplication, ensure that the template 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

Using mailbox classes to manage mailbox privileges

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 Email-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 screen to print a time-stamped list of all configured mailbox classes.

Getting there: **User → Mailbox Classes**

Creating and deleting mailbox classes

The method you choose to create a new mailbox class depends on whether you want the properties similar to an existing mailbox class, or whether you want to start with all CallPilot mailbox class defaults.

Note: You cannot delete a mailbox class if the mailbox has members.

Configuring mailbox classes

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 is 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 to suit the plans of your organization:

- 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.

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.

Tasks required to configure mailbox classes

- Display the mailbox class properties.
- Control the amount of resources used by the mailbox.
- Set call answering options.
- Set message delivery options.
- 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 Email-by-Phone feature is installed and mailbox owners must screen e-mail messages at any given time.
- 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.

- Control telecom charges by specifying the dialing permissions and restrictions for each feature enabled for mailbox class members.

ATTENTION

All supplied restriction permission lists (RPL) 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

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
- Email-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.

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 the 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 Email-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

Permitting mailbox class members to listen to e-mail messages over a phoneset

If Email-by-Phone capability is not installed on the CallPilot server, the corresponding check box is not included in your mailbox class options. The Mailbox Manager Web interface is the only way mailbox owners can configure Email-by-Phone preferences.

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.

Finding mailboxes, administrators, or directory entries

Search methods

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. You can specify a set of up to three search criteria, and base search criteria on information that is stored in the CallPilot database.
- 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 the Last Name link to display detailed information about a found CallPilot mailbox owner or administrator.
- Click the column name box to select or de-select all search results for deletion.
- Click the Delete Selected button to delete the mailbox owners or administrators indicated by a check mark.
- Click the Add button to add a mailbox owner or administrator that is missing from the group.
- 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.

Finding mailbox owners by name or mailbox number

When you must find a specific user by name, the quick user search is appropriate. After you create a search that successfully finds a specific group of users, save it for re-use.

Creating and using a set of 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.

Specifying the data element

The Search Criteria list provides data elements on which you can base search criteria. 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, and volume where 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.

Group label	Description
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.

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.

Getting there: **User → User Search → Advanced Search**

Adding mailboxes, one at a time

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)
- any shared distribution lists to which the mailbox is to be added (optional)

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

Using Auto-Add to add a group of mailboxes in a single operation

CallPilot Manager leads you through the steps required to add a group of mailbox owners to the CallPilot database.

You can also use Auto-Admin to create remote users, by assigning users to a template configured as a Remote User. Refer to the *Network Planning Guide* (555-7101-102) for further information.

Note: Do not use this feature during high traffic periods to avoid slowing server performance.

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

Note: The system assumes that the first row of your Excel worksheet is the header row — the row which contains the column headings. The system assumes that the second row of your worksheet contains your data. Ensure that the first row contains your column headings so that the system uploads all of your data, starting with the second row.

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.

Getting there: **User → Auto Add**

Using Auto-Delete to delete a group of mailboxes in a single operation

When a mailbox owner leaves the organization, you should remove the mailbox to prevent misuse by hackers. The Auto Admin Delete feature enables you to work more efficiently in a high-capacity system.

Using the same Excel spreadsheet used in Auto Admin Add - refer to "Information you need" on page 53. On the Excel spreadsheet, remove the appropriate users.

Note: If networking or NMS is configured on the system, the location name must be a column in the list. If the location name is not specified, only users from the prime location are deleted.

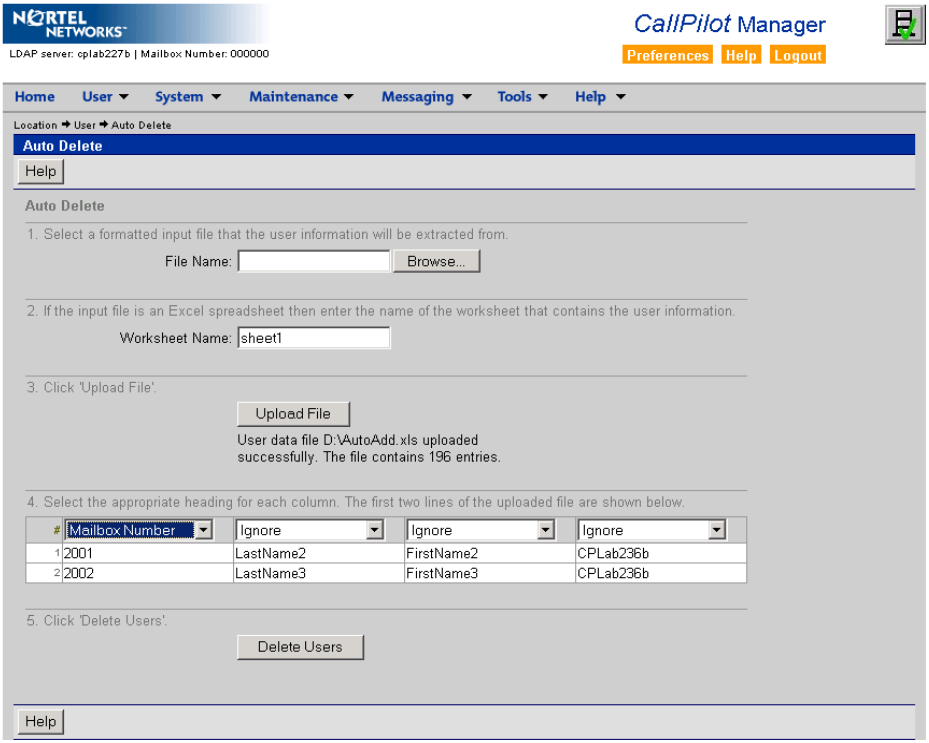
ATTENTION!

The delete cannot be undone. There is no undo, when the user is deleted they are removed from the system.

You access the Auto Admin Delete feature in the same way that you access the Auto Admin Add feature:

Getting there: **User → Auto Delete**

1. Use the **Browse** button to select a formatted input file that the user information is extracted from.
2. If the input file is an Excel spreadsheet enter the name in **Worksheet Name** dialog box.
3. Click **Upload File**
4. Select the appropriate heading for each column. (The first two lines of the uploaded worksheet are shown).
5. Click **Delete Users**.



Changing mailbox information

When a mailbox owner changes job functions, update his or her mailbox information as requested. Whenever a mailbox owner forgets a mailbox password, an administrator must reset it.

Re-enable a mailbox if it is automatically disabled. A mailbox is automatically disabled when it remains unused for too long, or when there have been to many consecutive unsuccessful attempts to log on.

Enabling or disabling Auto Logon to a mailbox

When enabled by the mailbox owner, Auto Logon allows a caller to automatically log on to the mailbox from a DN associated with the mailbox. To configure Auto Logon to a mailbox, your system may require a prefix to the external DN. If required, the prefix (for example, 9) entered in the field before the DN, is dependent on the configuration of your switch or system, or CallPilot system.

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 Auto Logon DNs are enabled in the user's profile, the user cannot enable Auto Logon from a phoneset.

Security feature

To prevent unauthorized access to a mailbox, CallPilot disables Auto Logon 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 Auto Logon from the phoneset.

Cautions

If a user complains that Auto Logon is not working when 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.

Changing individual mailbox properties

You may often need to change individual mailbox properties whenever mailbox owners request changes to their mailbox user properties.

Personal information

When a mailbox owner changes job functions, you must update the job title or department.

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.

Message blocking

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.

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, you can override the specification for that mailbox class member only.

Email-by-Phone voice gender

Mailbox owners who use Email-by-Phone to play their e-mail messages over the phoneset, may request either a male or female voice.

Preferred language

As new languages are installed on the system, users might request that they hear mailbox prompts in a different language. If the mailbox class specifies it, the mailbox owner's preferred language is also used for call answering prompts from the mailbox.

Busy line notification

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.

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.

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.

When you enable remote notification or add a mailbox owner 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 or the mailbox owner time

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. 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.

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 by means of Email-by-Phone or My CallPilot must have their account information specified in their user properties.

- 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 by means of Email-by-Phone.

Mailboxes with 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)

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 Mailboxes with fax deliveries and fax machine overflow page 61.

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 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.

Task summary

- Refer to the Switch Configuration Worksheet (see the *Installation and Configuration Task List*) 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
- 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.

- 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.
- Configure remote notification for all fax general delivery mailbox owners. (optional)

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 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 is 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 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

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 Task List* (555-7101-210).

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 sends 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.

Note: If an MWI DN is shared with a mailbox, the MWI will not indicate the appropriate status of either mailbox. Nortel recommends you do not configure a shared MWI DN that is also a CallPilot mailbox number.

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	

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 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 Task List* (555-7101-210).

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 the *Installation and Configuration Task List* (555-7101-210)).

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.

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 occurred. The message is tagged as urgent. After you receive a notification message, look at the Alarm Monitor to get more details. Nortel 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**

Chapter 5

Using Directory Synchronization

In this chapter

Overview

What is Directory Synchronization?

Businesses and corporations track their employees' phone numbers, department numbers and other necessary contact information. This data can be stored in a Microsoft product called Active Directory (AD.) Active Directory is Lightweight Directory Access Protocol (LDAP) compliant.

Typically the AD is synchronized with the corporation's Human Resource database as employees enter and leave the company or move departments. The CallPilot 4.0 Directory Synchronization feature automatically synchronizes the AD with CallPilot mailboxes.

Directory Synchronization applies to companies using a small network and a single CallPilot, as well as large corporations with a WAN and multiple CallPilot servers. Directory Synchronization reduces the time required to set up and maintain mailboxes.

The Directory Synchronization feature is configured through CallPilot Manager.

Example

- Company XYZ Inc. has an AD server that maintains employee information. The company purchases a new CallPilot server. Using Directory Synchronization, hundreds of mailboxes are added to the CallPilot server in one synchronization session, saving the administrator from spending time manually entering the information.
- A large corporation has an AD server containing thousands of users. As well, they have CallPilot servers located in various places throughout the corporation. With Directory Synchronization, a single administrator can add, update, and remove CallPilot users in multiple locations from a central AD.

Directory Synchronization can synchronize with an Active Directory running on Windows 2000 Server (Standard and Advanced Editions) or Windows Server 2003, Standard and Enterprise Editions.

Data is always driven from the Active Directory to CallPilot. The Active Directory is also referred to as the “external directory” in this document.

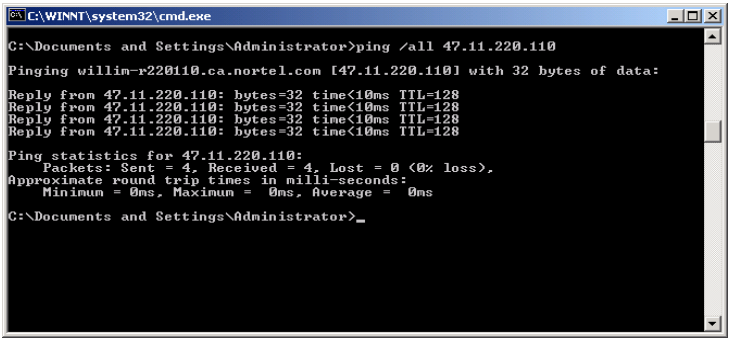
Defining the Active Directory requirements

Before you configure Directory Synchronization, you must ask the Active Directory Administrator for an administrator account which includes user name and password. The AD administrator must delegate control to this user account for the portion of the directory you are synchronizing, with the following minimum permissions:

- Read permissions to object class “users” (Windows 2000)
- Read permissions to object class “users” and “inetOrgPerson” (Windows 2003)
- Write permissions to the LDAP attribute “otherMailbox”, which has the display name “E-Mail Address (Others)”

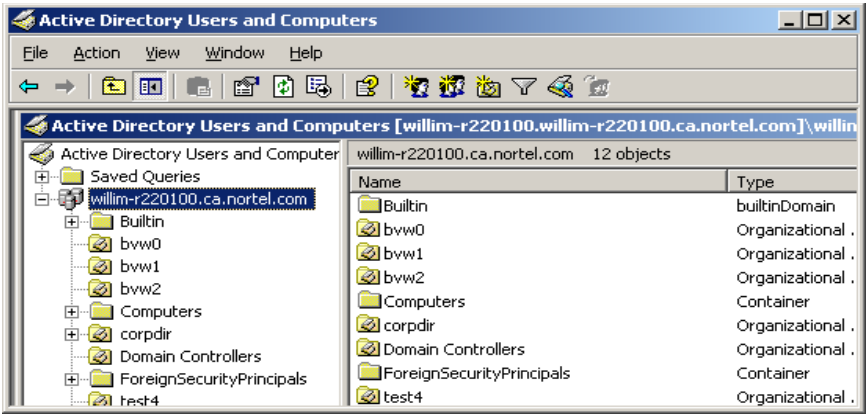
You require the following information about the Active Directory:

- **The FQDN**. This is the Fully Qualified Domain Name of the Active Directory server. The FQDN is usually the computer name plus the Domain Name System (DNS) suffix separated by dots. The easiest way to find this information is to ping the computer name. The figure shows the FQDN being returned as willim-r220110.ca.nortel.com.

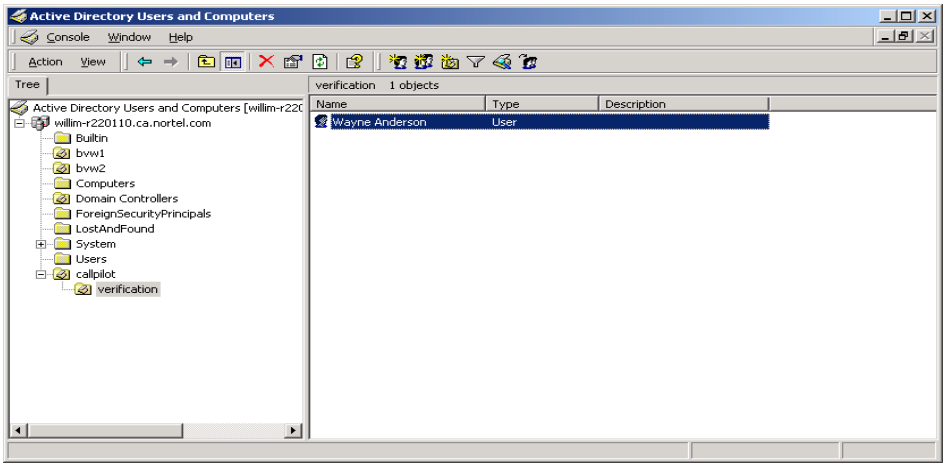


- **The LDAP suffix**. This is the base of the directory tree where the users exist. Usually the same as the Domain the AD is responsible for, with

"dc=" in front of each component. In the following figure, the LDAP suffix would be "dc=willim-r220100,dc=ca,dc=nortel,dc=com."



- **The User Name**. This user name is part of the user account given to you by the Active Directory Administrator. The user name is found in the Name column of the Active Directory users and computers screen.



- **The LDAP Port**. The default LDAP port number is 389.
- **The SSL Port**. The default SSL port is 636.

Using Directory Synchronization

Getting started

Only administrators with the Directory Synchronization privilege or full access rights can access this feature.

Configuring the Synchronization Agent is accomplished in four major steps. To run or schedule a synchronization task for the first time, follow these steps in sequence:

1. Changing the Local CallPilot Directory Connection Password
2. Configuring Directory Connections
3. Configuring Synchronization Profiles
4. Creating and Scheduling Synchronization Tasks

To change the local CallPilot Directory Connection password

The CallPilot Directory Connection uses a new, hidden account (mailbox number 010101) to log in and perform synchronization. This account has limited security privileges, and is locked until the password is changed. Once the password is changed, the account is enabled and you can proceed to configure the rest of the Directory Synchronization feature. To change the password, follow these steps:

1 Log on to CallPilot Manager. From the main menu, select **System → Directory Synchronization**.

Result: A dialog box appears indicating the requirement to set the password for the Local Server.

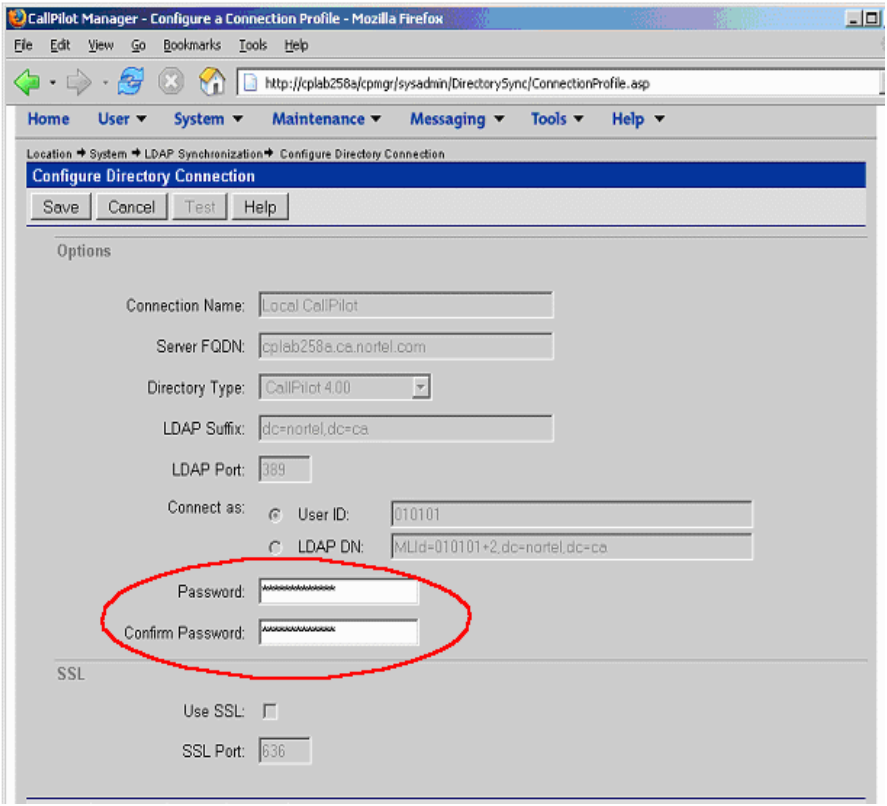
2 Click **OK** on the dialog box.

Result: The **Configure a Directory Connection Profile** screen appears. Only the password fields are available. The other fields have been set automatically and cannot be changed.

3 Enter your password in the **Password** and **Confirm Password** boxes and click **Save**.The password is saved, and the **Directory Synchronization Screen** appears. The local CallPilot connection now

appears under **Directory Connections** as a link. You may change the password at any time by clicking the link and repeating step 3. You are now ready to configure a Directory Connection.

Note: The password for the Local CallPilot Directory Connection account is not the same as the administrator or CallPilot password. The Local CallPilot Directory Connection is a unique password.



To configure directory connections

The Directory Connection contains the information required by the CallPilot Synchronization Agent to connect to the External Directory Server. You can configure up to five Directory connections. To configure a Directory Connection, follow these steps. Click on the **Help** button for more detailed information about each field.

1 From the Directory Synchronization screen, select **Configure Directory Connections** from the drop-down list.

Result: The screen displays the existing Directory Connections as links.

2 Click on **Add Connection**.

Result: The **Configure Directory Connection** page is displayed.

3 Enter the following information:

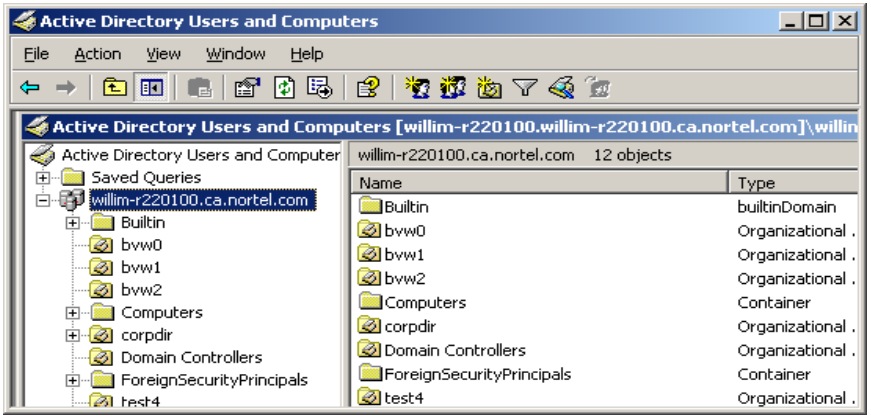
a. **Connection Name**: The Connection Name can be any name of your choice; you cannot leave this field empty.

b. **Server FQDN**: The FQDN of the external Server. Normally the computer name plus the Domain Name Server (DNS) extensions. See “Defining the Active Directory Requirements” page 73.

c. **Directory Type**: Choices are Active Directory 2000 or Active Directory 2003.

d. **LDAP Suffix**: If the LDAP suffix provided by the Active Directory administrator is the same as the Server FQDN this field can be left blank. Otherwise the LDAP suffix is determined by placing “dc=” before each component in the root of the external directory tree. For example:

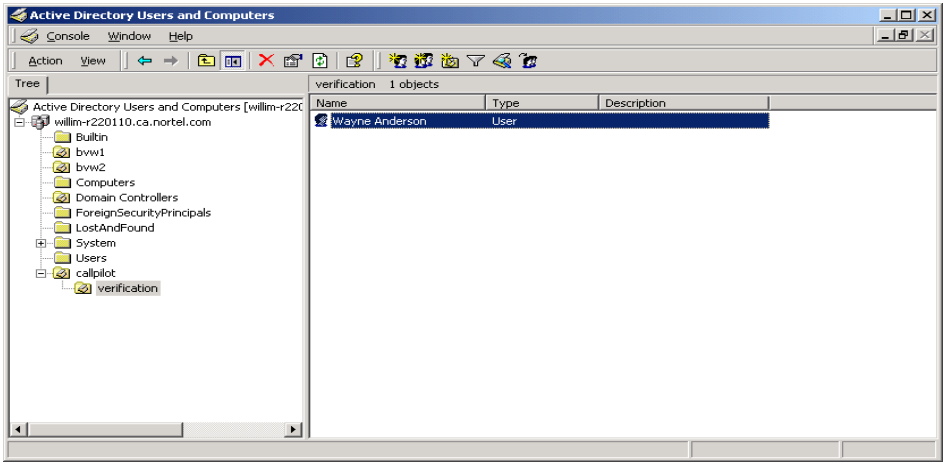
"dc=willim-r220100,dc=ca,dc=nortel,dc=com."



e. **LDAP Port**: Ask the Active Directory Administrator for the port number. The default is 389.

f. **Connect As**: If **LDAP DN** is selected, the **User Name** field is unavailable.

g. **User Name**: Directory Administrator level credentials. This is the user name given to you by the Active Directory Administrator. See "Defining the Active Directory Requirements" on page 73. If the User Account is not within the "Users" folder (refer to figure below), then **LDAP DN** must be selected in step "h".



h. **LDAP DN**: The LDAP DN must be used to authenticate using the LDAP protocol. The LDAP DN is automatically filled in as other fields are entered, and assumes that your account is in the “Users” folder. If your account is not in the “Users” folder, select the **LDAP DN** radio button and type in the LDAP DN information. In the above illustration your account exists in the verification organizational unit. Change the LDAP DN to:
“cn=wayne anderson,ou=verification,ou=callpilot,dc=willim-r220110,dc=ca,dc=nortel,dc=com.” (Refer to “Configure a connection profile” figure below Step 5.)

i. **Password and Confirm Password**: This is the password associated with the User Name or LDAP DN.

j. **Use SSL**: Select if communication to this directory is to be encrypted through SSL. Enabling SSL slows down the synchronization, but secures the connection.

Note: SSL is not enabled by default on AD. Your Active Directory administrator must set up Certificate Services and publish a valid certificate before Directory Synchronization or any other application can use SSL with AD.

k. **SSL Port**: Ask the Active Directory Administrator for the port number. The default is 636.

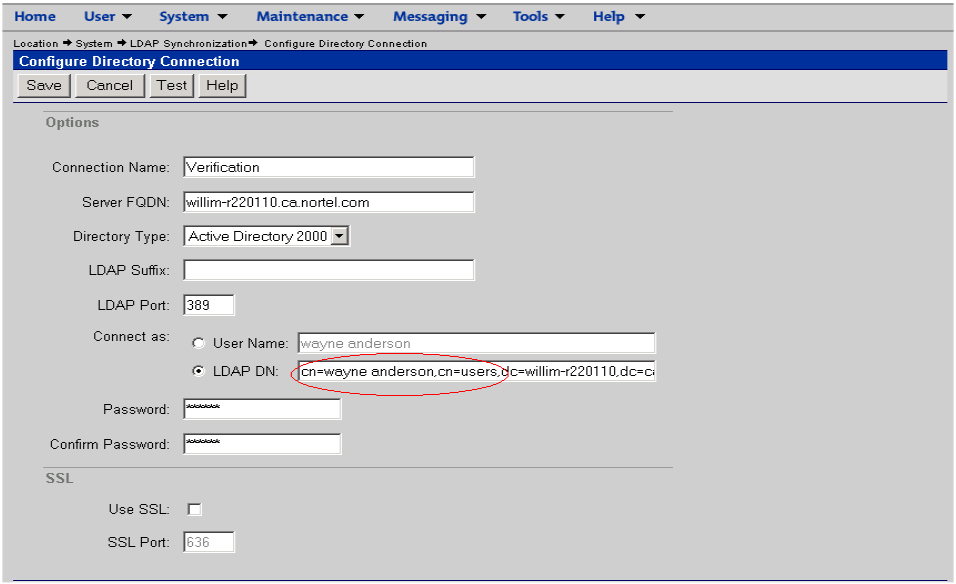
4 Click on the **Test** button.

Result: A pop-up dialog box informs the administrator whether the defined server can be contacted.

Note: If the test is unsuccessful, carefully check the information in each field.

5 Click **Save.**

Result: The Directory Connection is saved. The Directory Synchronization screen appears. The newly configured Directory Connection is displayed as a link on the screen.



To configure Synchronization Profiles

The Synchronization Profile contains the attribute mapping between CallPilot mailbox users and the external directory entries. You can define up to 50 Synchronization Profiles. You must define at least one profile before you can configure a Synchronization Task. To configure a Synchronization Profile, follow these steps:

1 From the Directory Synchronization screen, select **Create and Edit Synchronization Profiles** from the drop-down list.

Result: The configured profiles are displayed under Synchronization Profiles.

2 Click on the **Add Profile** button.

Result: The Configure Synchronization Profiles screen appears.

3 Enter or select the following information:

a. **Profile Name**: This can be any name of your choice; you cannot leave this field empty.

b. **Directory Connection:** There is at least one available connection.

- If no Directory Connection is defined, click on the **Add** button. The Directory Connection screen appears. See “Configuring Directory Connections” on page 76. Information on the Configure Synchronization Profiles screen is retained.
- To change any information in the selected Directory Connection, click on the **Modify** button. The Directory Connection screen appears. Edit the **Directory Connection**. Information on the Configure Synchronization Profiles screen is retained.
- Select the Organizational Unit from the drop-down list: This is the portion of the external directory that can be synchronized.

4 View the information under **Mapping**. There are default values for some of the attributes. Check with the Active Directory Administrator to ensure these attributes contain valid data. For example, ensure that the user’s phone numbers are stored under the **telephonenumber** attribute, if it is not then select the correct attribute.

Note: If the default values meet your requirements, proceed to step 7.

CAUTION

Caution must be observed when mapping attributes. Improper mapping can result in invalid mailbox information. For example, if the department number is inadvertently mapped to the given name, all given names could be overwritten by their department numbers.

5 Select the link for the **CallPilot attribute** you want to map or un-map.

Result: The Attribute Mapping screen displays.

a. From the drop-down list, select the **External Directory** attribute that you want to map from. If you want to remove the attribute mapping, select **not mapped**.

b. Select the appropriate **Transformation Rule**. This is only enabled for telephone numbers.

Example: Users' telephone numbers appear as 7 digit numbers, for example 343-8858. If you want the Callpilot mailbox number to be 8858, select "last 4 digits."

c. Click **Save.**

Result: The Configure Synchronization Profile screen appears. In the Mapping section, in the External Server Attribute column, the recently mapped attribute is displayed. The transformation rule will appear in the transformation rule column.

6 Repeat step 5 until all desired attributes are mapped.

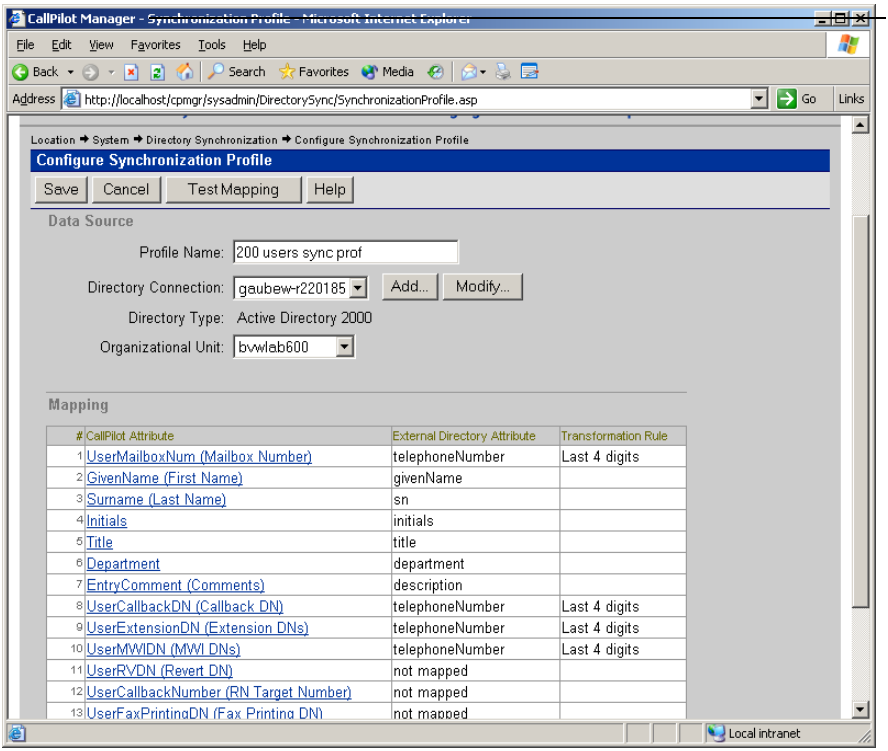
7 Click on the **Test Mapping** button.

Result: The Test Mapping screen appears. This screen displays the first five External Directory users and shows which data is mapped to which CallPilot attribute during synchronization.

- You can continue to edit the mapping until the test mapping button produces the desired results.

8 Click **Save** on the **Configure and Edit Synchronization Profiles** screen.

Result: The information is saved. The Directory Synchronization screen displays. The new Synchronization Profile is displayed as a link on the screen.



Configuring Synchronization Tasks

You can use the synchronization task to configure a new CallPilot system, or to update an existing system. If a user exists in the external directory, and not in CallPilot, the user is added as a new mailbox (provided the task filter criteria are satisfied). If there is a match between a CallPilot user and an

external directory user, the CallPilot user is linked to the external directory entry and is updated accordingly. Scheduling synchronization tasks to run weekly or monthly keeps the directory in synchronization and reduces your work load.

ATTENTION!

If multiple CallPilot users are synchronized with the same Active Directory user, the resulting link is invalid.

Note: If the Synchronization Task used to provision CallPilot is set to run with any recurrence (weekly or monthly), then any entries added to the external directory are added as new CallPilot mailboxes the next time the task runs.

To configure a synchronization task

1 From the Directory Synchronization screen, select **Review and Schedule Synchronization Tasks** from the drop-down list.

Result: The configured Synchronization Tasks appear as a link under Synchronization Tasks on the screen. If there are no tasks configured, this area is blank.

2 Click **New Task**.

Result: The Schedule Synchronization Task screen appears.

3 Enter or select the following information on this screen:

a. **The Task Name**. Type a name of your choice; you cannot leave this field empty.

b. **The Synchronization Profile**. Select a profile from the drop-down list.

- If you want to configure a new Synchronization Profile, click on the **Add** button. The Profile screen is displayed. You may now configure a new Profile without losing any information on the Schedule Synchronization Task screen.

- If you want to edit the selected Synchronization Profile, click on the **Modify** button. The Profile appears. You can edit the Synchronization Profile without losing any information on the Schedule Synchronization Task screen.

c. Select the Error Threshold:

- If you choose **Ignore Errors**, the Synchronization task runs to completion regardless of the number of errors.
- If you choose **Stop Task After**, the Synchronization task stops when the configured number of errors are reached.

d. Select the Log File type. The log file is generated when the task is running, and is available to the administrator: **Directory Synchronization > View History** the task history screen appears.

- **Basic** is chosen by default and is used during normal operation. Basic is a summary of performed operations and errors.
- **Detailed** gives more detail about the Synchronization Task. Detailed is usually used to diagnose problems or to send to the support organization.

e. Enter a task filter. This is an LDAP search filter to narrow the scope of the synchronization task. See “Defining a Task Filter” on page 90.

- Only entries matching this filter are synchronized. Enter the filter manually or use the **Insert Attribute** and **Insert Operator** drop-down lists to configure the filter.
- If synchronizing to multiple CallPilot servers from one external directory, you must ask the Directory Administrator to identify which external directory users should be linked to which server. This is accomplished by selecting an appropriate task filter. Also, ask the Directory Administrator if there is a unique attribute or can one be created.

4 Test the filter by clicking on the **Test** button.

Result: The Test Filter screen appears. You can set the number of entries to display.

Note: The number of entries displayed is controlled by the external server, and may not match the number configured on this screen.

5 Check the entries displayed in the Test Filter screen**.** Do this to ensure the filter is selecting the users you want to synchronize.

6 Determine how the task handles matching mailboxes:

- If you select the check box **only if last name is also identical**, and a CallPilot user is found with the same mailbox number as an external directory entry, but different last name, this entry is not synchronized during a synchronization task run.
- If you do not select the check box **only if last name is also identical**, and a CallPilot user is found with the same mailbox number, as an external directory entry, but different last name, this entry is synchronized, and the last name is changed in the associated CallPilot mailbox.

7 **Select the default Template from the drop-down list.** All users are assigned to this template unless Conditional Templates are configured in the next step. Only Local User Templates are available in this list. Administrators, Remote Users, and Directory Entry Users cannot be synchronized.

Note: You cannot create a new mailbox if the template includes administrative rights.

If you do not require any more than one template, proceed with step 9.

8 **Create Conditional Templates**. The Conditional Template overrides the default template if the filters match.

If the CallPilot system is using NMS, the location where the users are created is taken from the template. To automatically add users to different satellite locations, select Conditional User Templates as the appropriate template.

a. Click the **Add Template** button.

Result: The Conditional User Creation Template appears.

b. Enter a template description: This can be any description of your choice, for example, Accounting Department.

c. Select the desired template from the drop-down list.

Note: You cannot create a new mailbox if the template includes administrative rights.

d. Enter the desired filter in the **Used If** dialog box. See “Defining a Task Filter” on page 90.

Note: This filter is combined with the Task Filter to select a further subset of users.

e. Enter the number of entries you want to display.

f. Click on the **Test** button.

Result: The Test Filter screen appears. This screen displays the selected number of users matching the configured filter.

Note: The number of entries displayed is controlled by the external server, and may not match the number configured on this screen

g. If necessary, modify the test filter and repeat step “f” until you are satisfied with the results on the Test Filter screen.

h. Click **OK**.

Result: The Change Synchronization Task screen appears. The Conditional Template appears as a link on the screen.

9 Schedule a Task**.**

CAUTION

Nortel recommends that:

- you run Synchronization Tasks during off peak hours.
- a Synchronization Task is not scheduled when an archive or backup may be running. Directory Synchronization potentially changes the data that the archive backs-up.
- run back-ups and synchronizations on different days, or allow the synchronization to complete prior to starting the back-up.

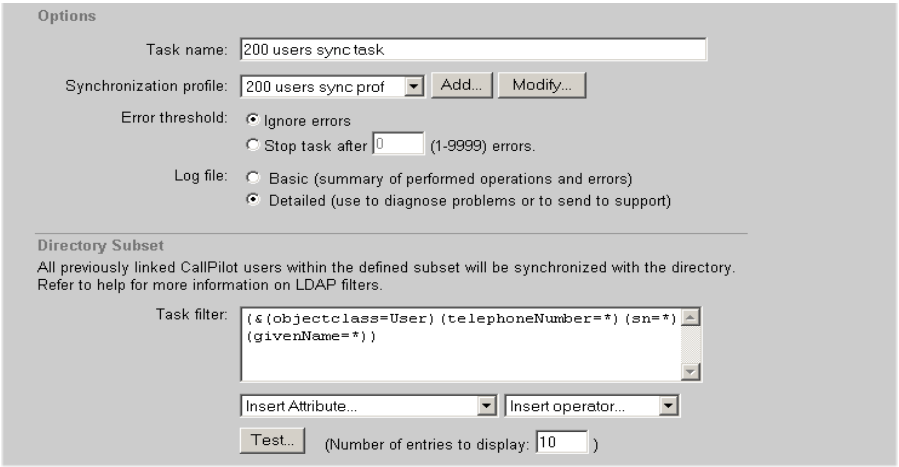
If you do not want this task to run on a schedule, leave the selection as Manually as Needed The schedule selections are unavailable. Proceed with step 10.

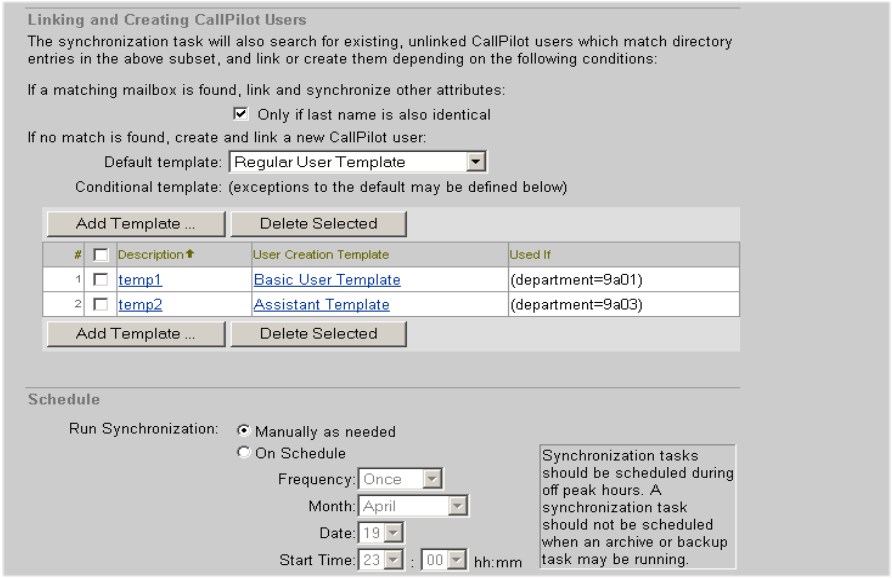
a. Select a frequency from the drop-down list. Choose from **Once, Weekly,** or **Monthly**.

b. Select a date and time from the appropriate drop-down lists.

10 Click **Save**.

Result: The task is saved. The Directory Synchronization screen appears. The task now appears as a link on the screen.




Linking and Creating CallPilot Users
The synchronization task will also search for existing, unlinked CallPilot users which match directory entries in the above subset, and link or create them depending on the following conditions:
If a matching mailbox is found, link and synchronize other attributes:
Only if last name is also identical
If no match is found, create and link a new CallPilot user:
Default template: Regular User Template
Conditional template: (exceptions to the default may be defined below)
Add Template ...
Delete Selected
Description User Creation Template Used If
1 temp1 Basic User Template (department=9a01)
2 temp2 Assistant Template (department=9a03)
Add Template ...
Delete Selected
Schedule
Run Synchronization:
Manually as needed
On Schedule
Frequency: Once
Month: April
Date: 19
Start Time: 23 : 00 hh:mm
Synchronization tasks should be scheduled during off peak hours. A synchronization task should not be scheduled when an archive or backup task may be running.

Defining a Task Filter

The task filter must be surrounded by parentheses, and must contain at least one attribute, operator, and value.

Attributes

There are many attributes within Active Directory, including the following three examples:

- sn (Surname)
- givenName (Given Name)
- telephoneNumber (Telephone number)

Operators

Logical Operators:

- & (AND) returns entries matching all specified filter criteria
- | (OR) returns entries matching one or more of the filter criteria
- ! (NOT) returns entries for which the filter is not true

Comparison:

- = (is equal to)
- >= (is greater than or equal to)
- <= (is less than or equal to)
- ~= (is like or sounds like)
- =* (exists)

Wildcard:

- * (Match 0 or more characters)

Examples of task filters:

Example 1:

(sn=a*)

In example 1, the task synchronizes all Active Directory users with last names beginning with “A.” This is a simple filter, which can produce problems. If the filter does not specify that a telephone number must exist, the task may attempt to synchronize an Active Directory entry without a telephone number. This is an error condition if you are mapping telephoneNumber to Mailbox Number.

Example 2:

(&(objectClass=user)(sn=*)(givenName=*)(areaCode=613))

In Example 2, the task synchronizes any user with the area code 613. This is more complex filter that ensures that that only entries with names and telephone numbers are synchronized. This filter might be used in a scenario with one Active Directory and multiple CallPilot servers where the area code determines the location of the user.

Example 3:

(&(objectClass=user)(sn=*)(givenName=*)(department >=4000)(telephoneNumber=*))

In Example 3, all users in department numbers 4000 and above are synchronized.

Example 4:

(&(objectclass=User)(|(telephoneNumber=4*)(telephoneNumber=5*))(sn=*)(givenName=*))

In Example 4, the task synchronizes any user with a telephone number beginning with 4 or 5.

To run a Synchronization Task

Before you run your first synchronization:

- Ensure that the data in the external directory is consistent and accurate.
- Synchronize one test user to ensure all settings are correct. You can do this by setting the task filter, so that only one user is selected.

Example How to define one user:

(telephonenumber=6133435479)

When a Synchronization Task is configured and tested, the task can be run at any time by following these steps:

1. From the Directory Synchronization screen, select **Review and Schedule Synchronization Tasks** from the drop-down list.

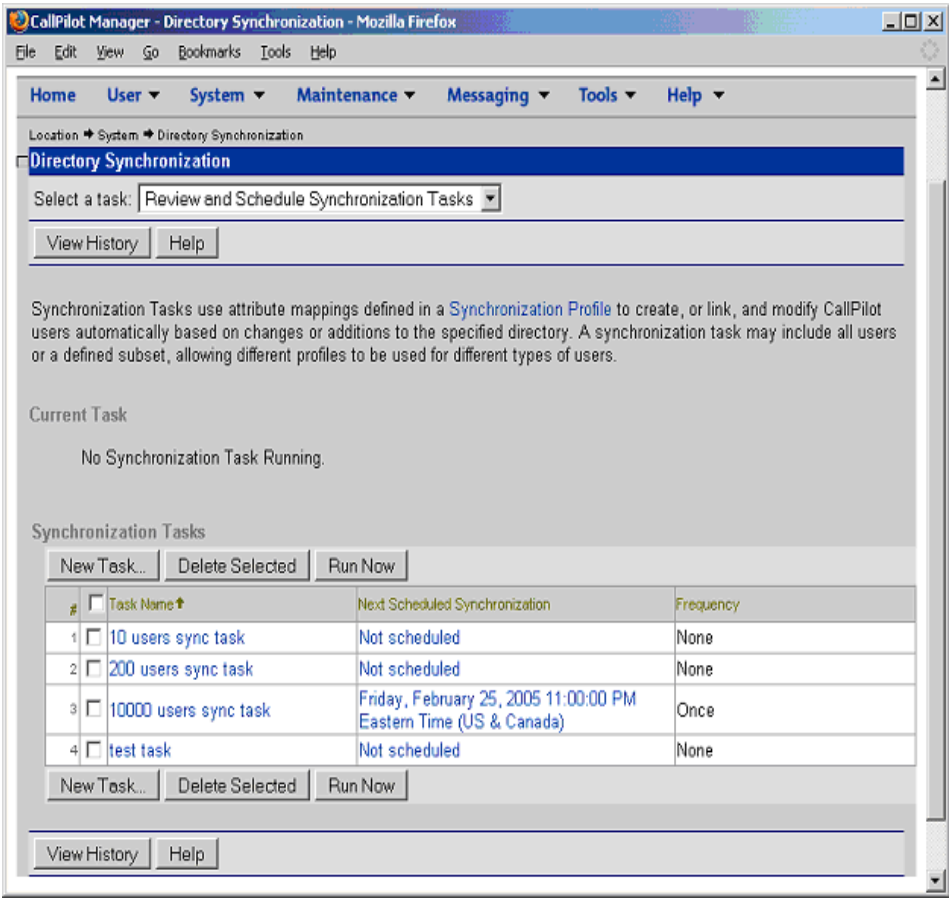
   Result: All configured tasks appear in the Synchronization Tasks area. If a task is currently running, the task appears under “Current Tasks”

2. Select the **check box** beside the task you want to run.

3. Click **Run Now**.

   Result: The task begins to run. The status is presented in real time under Current Task.

When the task is complete, be sure to check the log file to ensure there were no problems with the synchronization run. For more about the log file, see “Viewing the Log File” on page 93.



Viewing the Log File

A log file is generated during each synchronization run. Generally the last 60 log files are retained, though the oldest may be deleted earlier if the disk is greater than 90% full. The log file contains the following information:

- start and completion timestamp of the synchronization task
- the external directory that the log file synchronized with

- the number of records synchronized
- number of entries that failed to synchronize along with detailed information identifying which entries failed and why
- number of entries that were unlinked (due to the entry in the source directory being deleted)
- details of which records have been added, updated, or unlinked (Detailed Log only)

To view the log file

1 From the Directory Synchronization screen, select **Review and Schedule Synchronization Tasks** from the drop-down list.

Result: All configured tasks appear in the Synchronization Tasks area. If a task is currently running, the task appears under Current Tasks.

2 Click **View History**.

Result: The Task History screen displays.

3 Click on the hyperlink of the **Synchronization Task Log** you want to view.

Result: The Task Log is displayed.

Note: The log file location is usually D:\nortel\log\DirSync\. The specific log file can only be identified by date and time the job was started. Example file name - NMSync_Job2_05-23-05_01-29-57.log, generated on May 23, 2005 at 01:29 AM.

Note: For long log files there are links to assist navigation through the file.

Linking and Unlinking users from the User Details screen

A CallPilot administrator can manually associate an existing CallPilot mailbox with an external directory entry. Once linked, the pair is synchronized the next time any Synchronization Task is run (if the pair matches the associated profile).

To link a CallPilot user to an external directory

1 In CallPilot Manager, navigate to the details page of an existing user and scroll down to the **Mailbox** section.

Result: Under **linked to external directory**, the status is either linked or not linked.

If the status is linked, the **unlink** button is active. Unless you want to unlink this user and link to another external directory, there is no need to proceed. If the status in unlinked, the link button is active. Proceed to step 2.

2 Click on the **Link** button.

Result: The Link to external Directory screen appears.

3 From the drop-down list, select the **synchronization profile** you want to use to link this user.

4 In the **Quick Search** dialog box, enter the mailbox number, first name, or last name of the external directory entry. You can use the asterisk (*) as a wildcard. Click on the **Search** button.

Result: A list of matching entries is displayed in the results section of the screen.

5 Select the entry you want to link by selecting the box beside the given name. Scroll down if necessary, and click on the **Link** button.

Result: The user is synchronized and their status now shows linked.

To find and delete unlinked mailboxes

If an external directory entry is deleted, the next time a synchronization task is run, the link between that entry and the corresponding CallPilot mailbox is broken. In this case, the CallPilot mailbox must be deleted. To find and delete these unlinked mailboxes, follow these steps:

1 From the CallPilot Manager screen, navigate to User Search, then select **Advanced Search**.

Result: The Advanced Search criteria selections are displayed on the screen.

2 In the first **Search Criteria** drop-down list, select **Date unlinked from external directory**.

3 Select an Operator and Value from the drop-down lists.

4 Click on the **Search** button.

Result: A list of users matching the search criteria appears.

5 Delete the appropriate users.

Using the Active Directory Extension

The Active Directory extension comes with the Applications CD. For installation instructions, see *Software Administration and Maintenance (555-7101-202)*.

Note: The Active Directory Extension can NOT be installed on the CallPilot server.

Note: If a mailbox user exists on more than one CallPilot system, do not use the Active Directory Extension to update the user's mailbox.

The Active Directory Extension is used by the Active Directory Administrator to:

- Create a new CallPilot user.
- Link with an existing CallPilot user.
- Delete an existing CallPilot user.
- Unlink an existing CallPilot user.
- Define CallPilot servers that are used for the above operations.

Before you use the Active Directory extension, the Directory Connection and Profile must be configured on the CallPilot server.

To create a new CallPilot user from the Directory Extension

1 From the Active directory user and computer screen, right click and select the properties of the user.

Result: The Active Directory user's property page displays.

2 Click on the **CallPilot** Tab.

Result: The screen displays the user's status. In this case, the Create and Link buttons are active.

3 Click on the **Create** button.

Result: The **Create CallPilot User** dialog appears.

- *If you have previously used the Active Directory extension*, the Server drop-down list displays the server name. Continue to step 4.
- *If this is the first use of the Active Directory extension*, the system displays a prompt and the Server drop-down list displays <undefined>. To define the CallPilot server, follow these steps:

a. Click on the **Servers** button.

Result: The CallPilot Servers dialog displays.

b. Click on the **Edit** button. The import and export button are discussed later.

Result: The CallPilot Server Properties screen displays.

c. Enter the information in the appropriate fields. This information is found in the Local CallPilot link on the **Configure Directory Connections** screen in the CallPilot server.

d. Click on the **Validate** button.

Result: A dialog box appears indicating success or failure.

- If validation is unsuccessful, check the Directory Synchronization configuration in the CallPilot server, and correct the problem before continuing.

e. Click **OK**.

Result: The CallPilot Server appears in the CallPilot Servers dialog box.

f. Click **OK**.

Result: The Create CallPilot User screen appears.

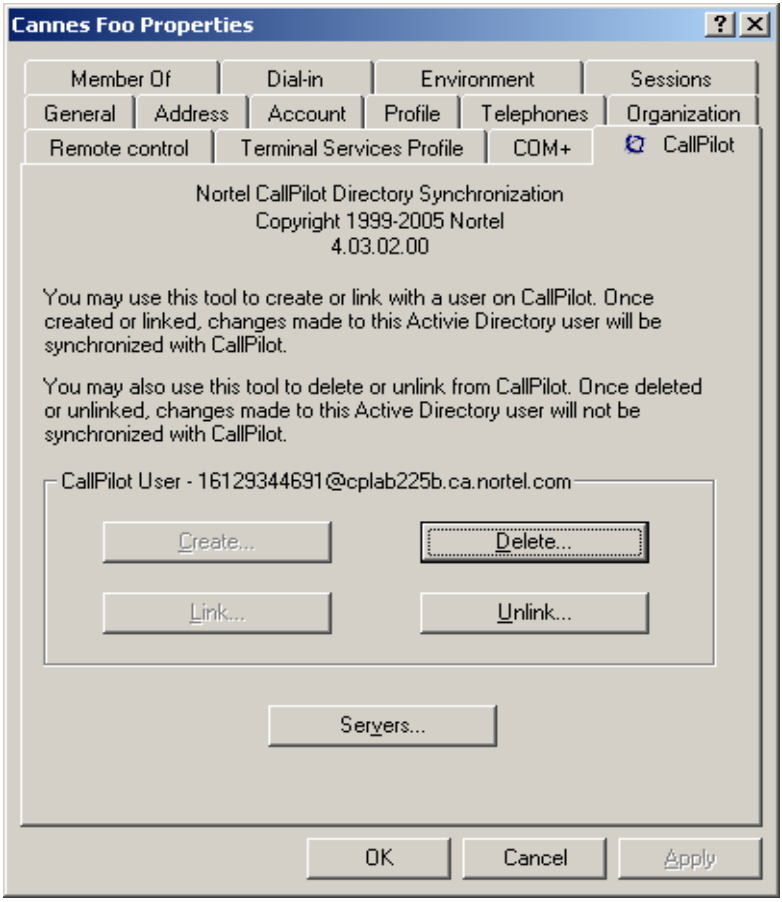
4 From the drop-down menus on the **Create CallPilot User** screen, select the desired Server, Synchronization Profile, and Template.

5 Click on the **Create** button.

Note: You cannot create a new mailbox if the template includes administrative rights.

Result: The user is created and linked. The Delete and Unlink buttons are active. The user's address appears above the Create button in the following format:

<SMTP\VPIM network shortcut><Mailbox>@<FQDN of the CallPilot Server>



To link to an existing CallPilot user

1 From the Active directory screen, right click and select properties of the user you want to link.

Result: The active Directory user's property page appears.

2 Click on the **CallPilot** tab.

Result: The screen appears the user's status. In this case, the Create and Link buttons are active.

3 Click on the **Link** button.

Result: The Link CallPilot User dialog box appears. If the CallPilot server is not defined, click on the **Servers** button, and follow steps 3 b to e under “Creating a new CallPilot User from the Directory Extension” on page 96.

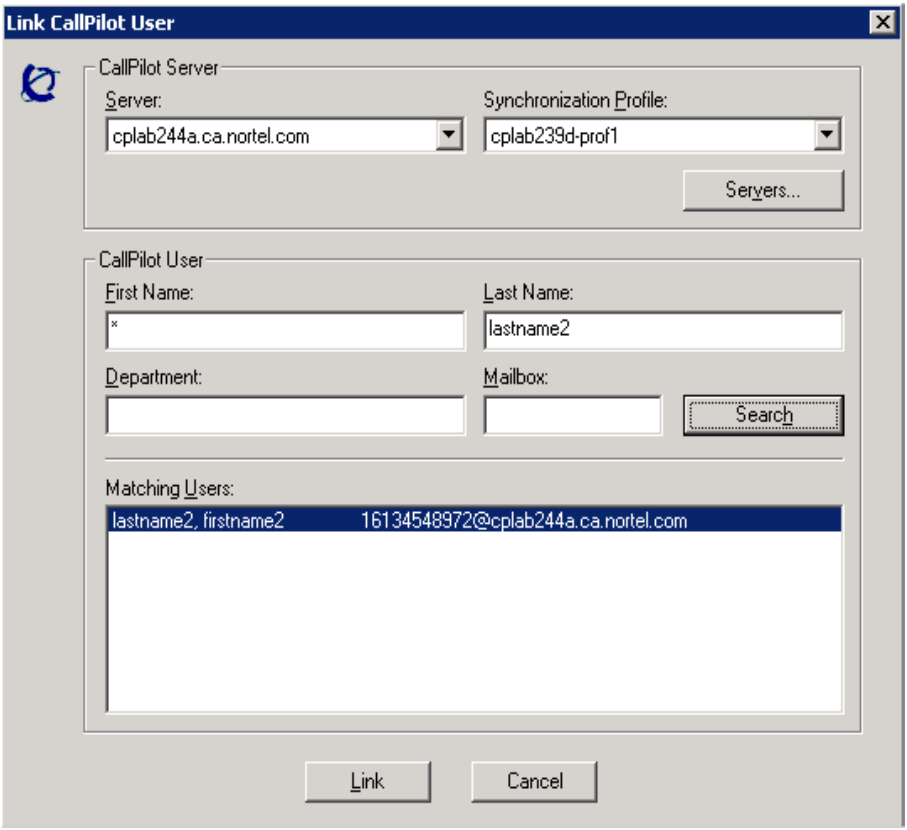
4 Select the desired Server and Synchronization Profile from the drop-down lists.

5 Enter enough Information in the **CallPilot User** fields to locate the user with a search, click on **Search**.

Result: All matches to the search appear in the Matching Users box.

6 Highlight the user you want to link, and click on **Link**.

Result: The user is created and linked. The Delete and Unlink buttons are active.



To unlink an existing CallPilot user

1 From the Active directory screen, right click and select properties for the user you want to unlink.

Result: The active Directory user's property page appears.

2 Click on the **CallPilot** tab.

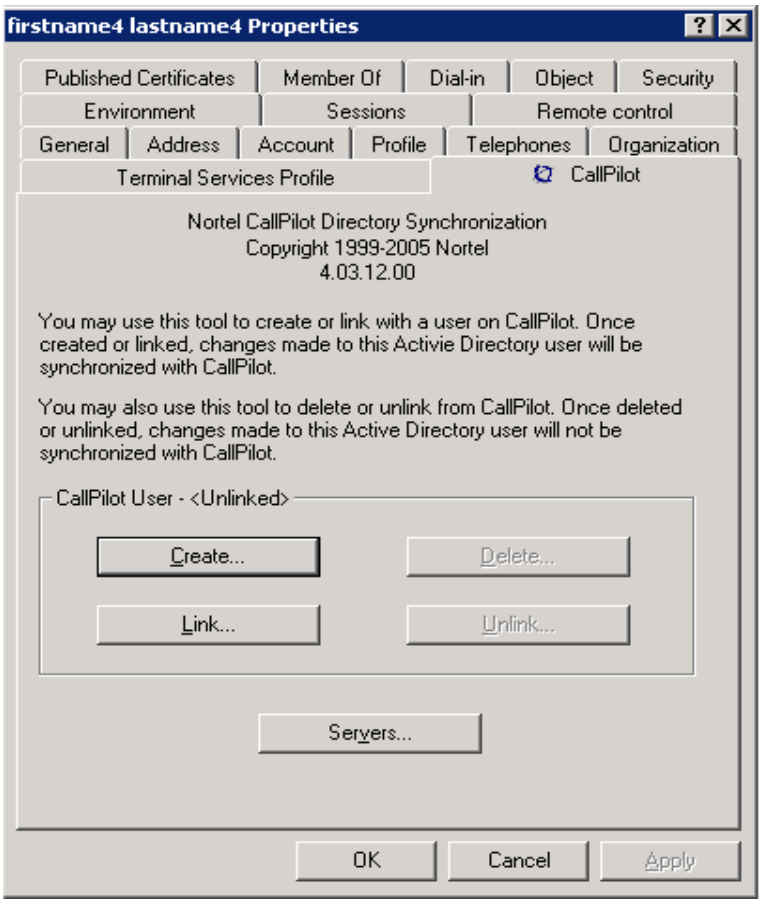
Result: The screen displays the user's status. In this case, the Delete and Unlink buttons are active.

3 Click on the **Unlink** button.

Result: A dialog box appears, requesting that you confirm this action.

4 Click on the **Unlink** button.

Result: The user is unlinked. No changes are made to this user in any future Synchronization runs until linking the user again.



To delete a linked CallPilot user

CAUTION

This action deletes the CallPilot user's mailbox, and all messages are lost.

1 Click on the **CallPilot** tab.

Result: The screen displays the user's status. In this case, the Delete and Unlink buttons are active.

2 Click on the **Delete** button.

Result: A dialog box appears, requesting that you confirm this action.

3 Click on the **Delete** button.

Result: The user is deleted. No changes are made to this user during any future synchronization runs until the user is linked again.

To import or export CallPilot server settings

You can use the Import and Export buttons on the CallPilot Servers dialog box to read in or write out CallPilot server credentials. Server credentials are read from or written to a text file that can be used to pass information between two different computers running the Active Directory extension.

1 From the Active directory screen, right click and select properties for any user.

Result: The active Directory user's property page appears.

2 Click on the **CallPilot** tab.

Result: The screen displays the user's status.

3 Click on the **Servers** button.

Result: The CallPilot Servers dialog box appears.

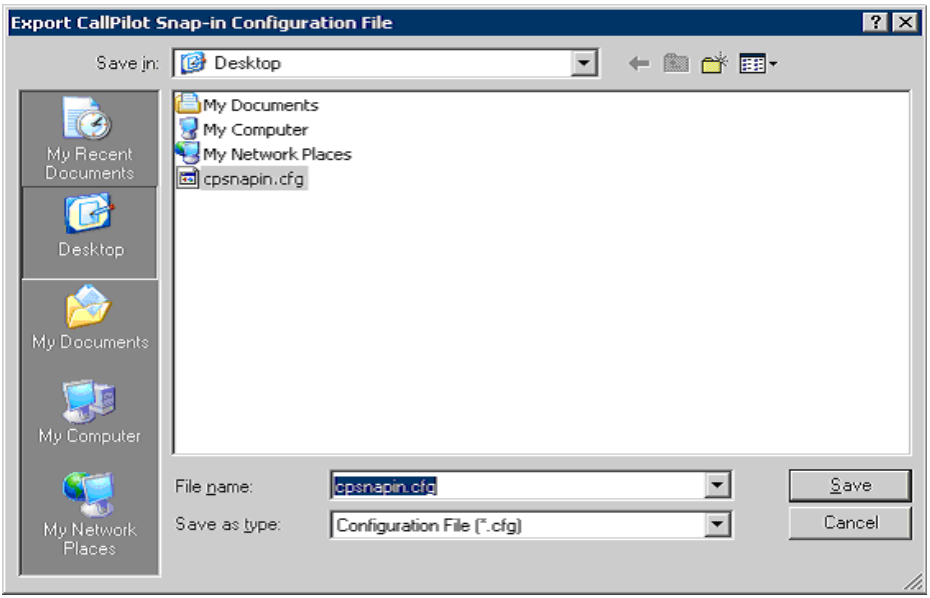
To export Server Settings: (The Administrator mailbox and password are encrypted when exporting server settings.)

a. Highlight the server you want to export, and click **Export**.

Result: The Export CallPilot Snap-in Configuration file dialog box appears.

b. Select the path and name of the file, and click **Open**.

Result: The file is saved as a .cfg file in the selected location. The file can now be copied to another Active Directory server.



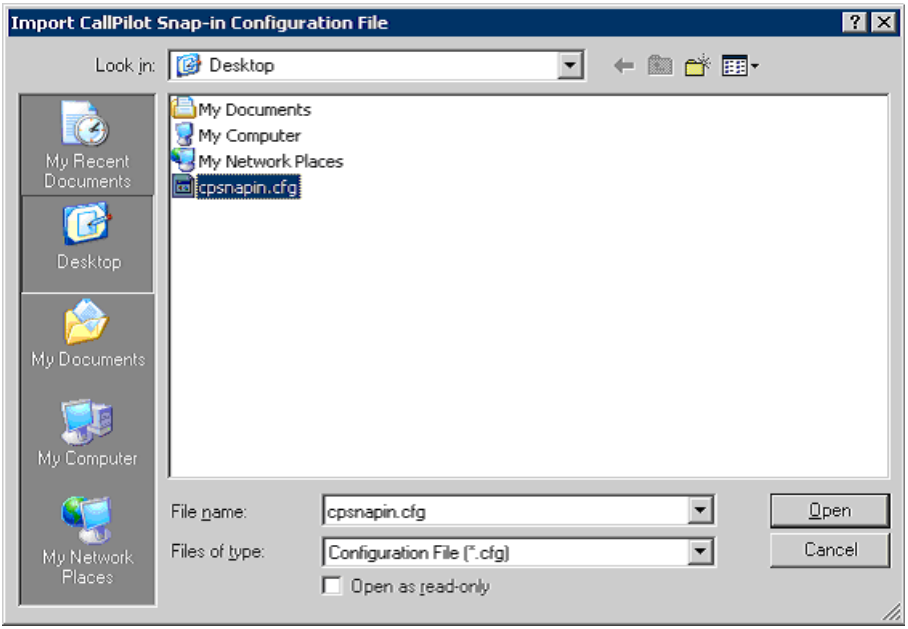
To import Server Settings:

a. Click **Import**.

Result: The Import CallPilot Snap-in Configuration file dialog box appears.

b. Highlight the .cfg file you want to import, and Click **Open**.

Result: The servers now appear in the CallPilot Servers dialog box.


Import CallPilot Snap-in Configuration File
Look in:
Desktop
My Recent Documents
Desktop
My Documents
My Computer
My Network Places
My Documents
My Computer
My Network Places
cpsnapin.cfg
File name:
cpsnapin.cfg
Files of type:
Configuration File (*.cfg)
Open as read-only
Open
Cancel

Chapter 6

Configuring dial-up access to the CallPilot server

In this chapter

Remote control of the server with pcAnywhere

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 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	Yes	Yes
2 Configuring the pcAnywhere client for dial-up to the CallPilot server	Yes	Yes
3 Creating the Dial-Up Networking connection profile	No	Yes
4 Establishing a connection using Dial-Up Networking	No	Yes
5 Taking remote control of the CallPilot server	Yes	Yes
6 Optimizing remote host response during a pcAnywhere session	No	Yes
7 Ending a dial-up connection	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 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 TCP/IP configuration information.

Configuring pcAnywhere on a personal computer

About pcAnywhere

One licensed copy of the pcAnywhere 11.0 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 11.0 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

Installing pcAnywhere on the remote personal computer

Nortel 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.

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

Getting there: **Windows Start → Programs → Symantec pcAnywhere**

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

Configuring pcAnywhere for dial-up to the CallPilot server

To connect to the CallPilot server, first create a pcAnywhere remote control connection to the server. For specific instructions on configuring the pcAnywhere client, refer to the Symantec pcAnywhere documentation.

If you are using pcAnywhere on a remote personal computer, establish a dial-up connection to the server. If you are using pcAnywhere on a personal computer that is on the same LAN as the CallPilot server, take remote control of the CallPilot server.

Restarting the server using pcAnywhere

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

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

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

Restarting CallPilot server remotely without using pcAnywhere

If pcAnywhere is not installed or not available, use HyperTerminal software to establish a connection. HyperTerminal is installed on the computer with the Windows operating system. HyperTerminal enables you to use a modem to connect to a remote computer even if it is not running Windows. After a HyperTerminal connection is configured, it becomes part of Windows Accessories.

Task summary

- Configure the HyperTerminal connection to the CallPilot server.
- Configure the modem ports.
- Edit the Host file to establish a connection with the server.

Information you need

- the country or region in which the CallPilot server is located
- the 10-digit telephone number of the CallPilot server
- the dialing rules for the location if using a laptop at a new location
- the port number to which the personal computer modem is attached

Getting there: **Windows Start → Programs → Accessories → Communications → HyperTerminal**

Dial-up networking

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 Routing and Remote Access Service (RRAS) 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.

The RRAS and pcAnywhere 11.0 software are installed on the CallPilot server at the factory. No on-site configuration is required.

Creating the Dial-Up Networking connection profile

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

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

You need to know the following information:

- the server telephone number
- the server IP address

Establishing a connection using Dial-Up Networking

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 Dial-Up Networking connection is not required.

Before you begin

- Ensure that you have created a server connection profile.
- A user ID and password are required to log on to the 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).

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

- Start CallPilot Manager.
- Use pcAnywhere to control the server as you perform administrative tasks.

ATTENTION

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

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

Chapter 7

Security recommendations

In this chapter

Secure Sockets Layer

Secure Sockets Layer, or SSL, is a protocol developed for transmitting private documents over the Internet. SSL uses a private key to encrypt data that is transferred over the SSL connection. SSL is supported by both Internet Explorer and Netscape Navigator. By convention Universal Resource Locators, (URLs) that require an SSL connection start with “https” instead of “http.”

Connections to the CallPilot server must be encrypted using SSL. There are three supported protocols; LDAP, SMTP, and IMAP. For each protocol there is a separate SSL check box to enable SSL on CallPilot server. The check boxes are:

- Enable LDAP with SSL port
- Enable IMAP with SSL port
- Enable SSL for incoming SMTP sessions

These settings affect the desktop client and user interface. If SSL is not enabled, at login, the user receives an error dialog box.

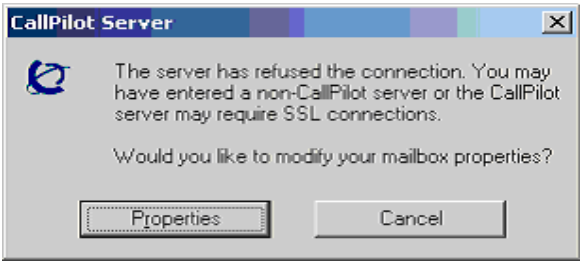
Require SSL feature

A new feature called Require SSL is introduced in CallPilot 4.0. The Require SSL feature enables CallPilot server to force all clients to use SSL connection when connecting using a specific protocol. There are three separate Require SSL check boxes for IMAP, SMTP, and LDAP protocols. When selected the IMAP, SMTP, or LDAP connections to the CallPilot server must be encrypted through SSL and the corresponding ports set to their equivalent. The check boxes are:

- Require SSL under LDAP section
- Require SSL under IMAP section
- Require SSL for Incoming SMTP sessions

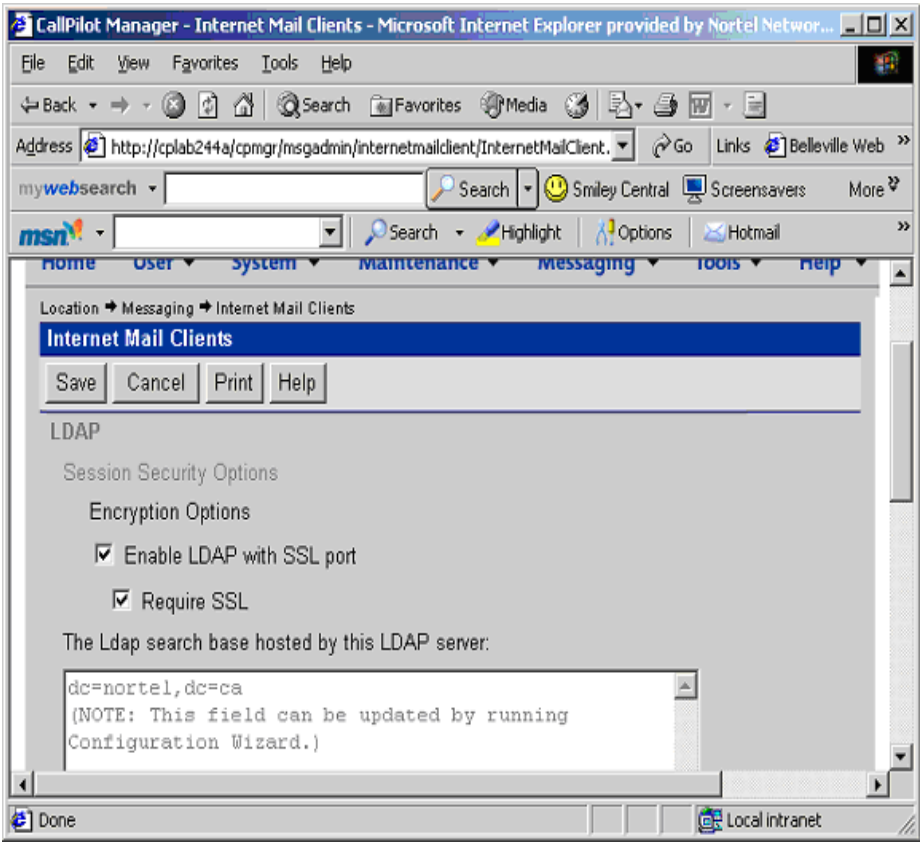
Require SSL setting affects the user interface of the desktop clients (integrated and non-integrated) and My CallPilot. When the check boxes are selected, the user receives an error as if the SSL has not been enabled for the specific protocol based on the request. IMAP is used to retrieve CallPilot messages, SMTP is used to send CallPilot messages, andLDAP is used for login (for My CallPilot) or on a request for Address Book, PDL, or SDL for all clients.

For integrated clients, an error message is received if SSL is forced on the server side but SSL has not been enabled on the client side:



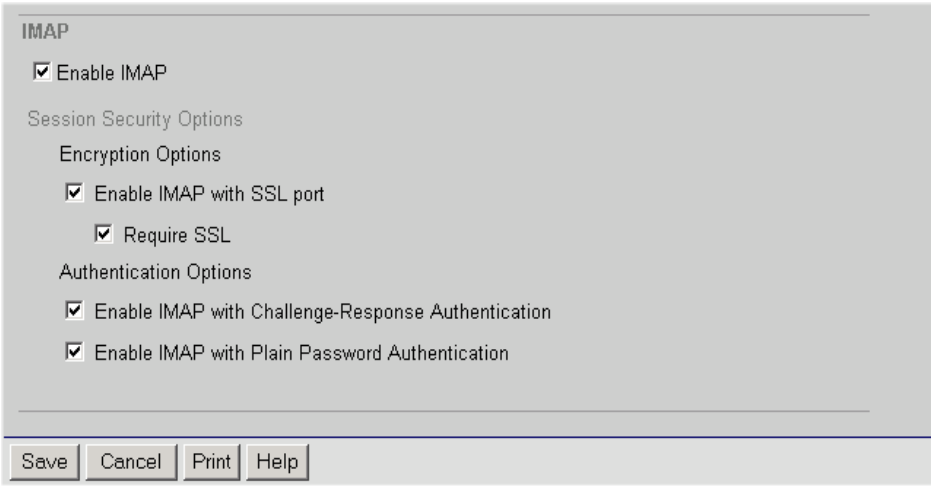
Configuring SSL settings from CallPilot manager

1 To Configure SSL Settings for LDAP protocol **CallPilot Manager→ Messaging→ Internet Mail Clients→ LDAP section**.

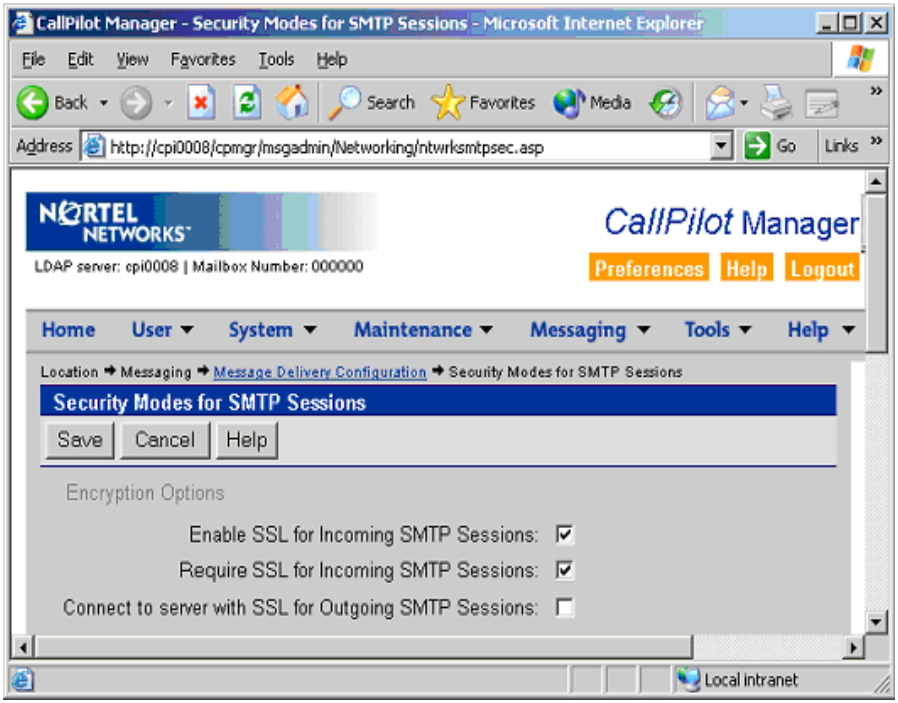


2 To configure SSL settings for IMAP protocol **CallPilot.**

Manager→Messaging→ Internet Mail Clients→ IMAP sessions



3 To configure SSL settings for SMTP protocol **CallPilot Manager→ Messaging→Message Delivery Configuration→Secure Modes for SMTP sessions.**



CallPilot security recommendations

- 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 the *Installation and Configuration Task List* (555-7101-210).
- Ensure that all CallPilot backup tapes are physically secured.
- Ensure that all Windows 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 the *Installation and Configuration Task List* (555-7101-210).
- 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 by means of 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 LAN firewall.
- Install and configure one of the Nortel supplied third party antivirus solutions.

ATTENTION

Do not install third-party antivirus software unless approved by Nortel. Refer to the *CallPilot Support for Antivirus Applications* bulletin for Nortel approved software.

- When you initiate a dial-up 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 needed to enable a dial-up connection for remote maintenance of the server.

Securing the premises

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 allow employees to decide who can come in and when.
- Review the “Site Inspection Checklist” in the *Installation and Configuration Task List* (555-7101-210).

Securing equipment

Set up a security policy to identify the measures 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.
- Keep track of keys or badges that are used to gain entry. When employees leave your company, cancel their access privileges.
- 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 beyond a certain amount.

Cabling and wiring

Secure cables and wiring by the following:

- Plan wiring runs, and make them secure against unauthorized 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 wiring system can be tapped. Shield wiring leading from a computer to the building wiring.

Remote personal computers

Protect remote personal computers by the following:

- Use power-on passwords that require a user to enter a password before the system starts. This prevents 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

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.
- Check file folders that are being thrown out for papers that might have been left in them.
- Keep network diagrams locked up. Shred any old network diagrams (that can show where routers are or which ports are blocked) before throwing them out.

Monitoring suspicious activities

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.

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
- a report generated in Reporter indicates unusual traffic or usage patterns

You can monitor

- internal and external telephone numbers, calling line IDs (CLID) 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 generated alarms 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

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.
55751	Failed login attempt to a mailbox from a 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 CLID are unknown.
55758	Successful login to a mailbox that is being monitored by the Hacker Monitor. The Calling Line ID is known.

Event number	Description
55759	Successful login to a mailbox that is being monitored by the Hacker Monitor. The Calling Line ID is unknown (Calling DN field is empty).
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 CLID 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. Calling Line ID unknown.

Monitoring options

You can specify individual mailboxes to track suspicious thru-dialing activities, logon attempts, or both. You can also specify a monitoring period.

To monitor mailboxes

1 On the CallPilot Manager toolbar, navigate to Messaging > Security Administration.

2 In the Mailboxes section, click either Logins or Thru-dials.

3 Enter the time you would like monitoring to occur.

4 *If you would like to monitor all mailboxes*, select *All.*

Result: All mailboxes are monitored.

If you would like to monitor specific mailboxes:

a. Select *Selected*.

Result: The Add and Delete buttons are enabled.

b. Type in a selected mailbox to be monitored.

c. Click Add.

Note: To remove a mailbox entry, highlight the entry and click delete.

5 Click Save to enable the changes.

Viewing the details for a specific event or return code

You can click the Event in the System/Event Browser to open the Event Code Help. If the help does not automatically display the desired information, click the Index tab in the left pane of this help file and type the event or return code as the keyword to find. The code is displayed in the index list, and when you click the code in the index list, the right pane refreshes to display the details for the specified event or return code.

Monitoring internal and external activity by calling line ID

When a call comes in to the system, CallPilot keeps track of the 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. 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 DN monitored by Hacker Monitor.
55751	Failed login attempt to a mailbox from a 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.

How to respond to alarms

If a specific mailbox is being targeted, determine if the mailbox is in use.

- If the mailbox 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
- for the entire day, or for a specified time period

To monitor CLIDs

1. On the CallPilot Manager toolbar, select Messaging > Security Administration.
2. Under the CLID section, click the checkbox *Monitor CLIDs for All Mailbox Logins and all Thru-dials on System.*

   Result: The Add and Delete buttons are enabled.
3. Select the times when you would like the Hacker Monitor active.
4. Enter the phone number (DN) you would like to monitor in the Internal or External box and click Add.
5. Click Save.

   Result: The entered DN is now activated and will be monitored.

Monitoring suspicious SMTP activity

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 screen 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 monitoring works

When CallPilot detects repeated unsuccessful authentication attempts (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 through the 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 activities 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.

To monitor SMTP/VPIM

1. On the CallPilot Manager toolbar, navigate to Messaging > Security Administration.
2. Under the SMTP/VPIM section, click the checkbox *Enable Monitoring activities.*
3. Click Add.
4. Select Activity Type (IP Address, FQDN or User ID)
5. Enter a value for your selected activity type and then click Save.

   Result: The Security Administration screen displays with your added entry under Activities to Monitor.

   Note: If you would like to delete or disable any of these activities, check the box next to the activity and click on Delete or Disable.

Monitoring custom application SDNs

You can monitor specified custom applications to track suspicious thru-dialing activities. After you have determined the cause of suspicious activity and have resolved the problem, remove the SDN of the corresponding application from the monitoring list.

Note: An event code is generated each time there is thru-dialing activity from a custom application SDN.

Monitoring options

You can monitor

- all applications for suspicious behavior, or you can specify certain applications to be monitored
- applications for the entire day, or for a specified time period

Getting there: **Messaging → Security Administration → Application Builder settings**

Configuring mailbox security

When you set up your CallPilot system, address the following issues:

- 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.
- 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 based on usage.

Issues and recommendations

Hackers often use corporate systems to pay for services accessed through 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.

Hackers look for signs that a mailbox is unused. Nortel 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.”
- Ensure that aged messages are automatically deleted from mailboxes.
- When you create new mailboxes prior to immediate use, defer access to the new mailboxes.

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 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.

Strong passwords for user accounts

Strong passwords use upper and lower case characters, numbers, and symbols to increase CallPilot security for the Administrator, NGenSys, NGenDist, and NGenDesign Windows accounts. Running the Configuration Wizard for the first time checks the accounts for the default password and if found, forces you to change the password.

ATTENTION

Nortel recommends the use of strong passwords. Strong passwords are enabled by default in CallPilot to provide increased system security.

Creating a strong password

Example of a strong password: J*p2le04>F

A strong password must:

- be at least 6 characters
- not use a complete dictionary word
- not contain your user name, real name, or company name
- be significantly different from previous passwords (for example, passwords that increment are weak; e.g., Password1, Password2, Password3)
- include characters from at least three of the following categories

Categories	Characters
upper case characters	A, B, C …
lower case characters	a, b, c …
numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
symbols found on keyboard	‘ ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : “ ; ‘ < > ? , . /

Note: Passwords that contain a space are accepted by CallPilot 4.0. Spaces are only place holders and not classed as numbers, letters or symbols.

Changing global mailbox password options

If the mailbox password defaults shipped with CallPilot do not adequately address the security needs of your organization, change them.

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

Getting there: **Messaging → Security Administration → Passwords settings**

Controlling access to mailboxes

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 to re-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.

Ensuring the use of a personal verification

Hackers look for signs that a mailbox is unused. Nortel 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.

Getting there: **User → User Search → User Detail page → Greetings settings**

Restriction permission lists

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. Using restriction permission lists (RPL) ensures that your organization does not incur unauthorized toll charges.

Each RPL consists of a restriction code list and a permission code list.

An 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**

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:

- Use CallPilot Manager Advanced Search to list the mailbox classes that allow external Call Sender.
- 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.

- 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.
- 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.
- If there are any mailbox classes left, determine if there are any which should permit off-switch dialing of any kind.
  - 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:

- Use CallPilot Manager Advanced Search to list the mailbox classes that allow mailbox class owners to specify an off-switch revert DN.
- 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.
- Ensure that the long distance 2 RPL is customized appropriately.
- 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.
- Ensure that the long distance 1 RPL is customized appropriately.
- 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.
- Ensure that the local RPL is customized appropriately.

- 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.
  - 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:

- Use CallPilot Manager Advanced Search to list the mailbox classes to allow mailbox class owners to send messages over the public network.
- 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.
- 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.
- 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.
- 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.
  - If so, list each special restrictions required and create one or more RPLs that block only the restricted calls.

Customizing RPLs

Customizing RPLs allows you 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.

ATTENTION

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

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.

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 RPL features such as the following:

- external call sender
- automated attendant services
- AMIS Open Networking

Customizing the on switch RPL to enable thru-dialing to other on-switch DNs

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.

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, and 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**

Customizing the local RPL to enable off-switch dialing

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 fails to the revert DN, callback DN, and MWI DN.

Getting there: **Messaging → Restriction Permission Lists → Local RPL**

Customizing the long distance RPLs

Customize the long distance 1 RPL to permit CallPilot to call domestic long distance.

Customize the long distance 2 RPL to enable CallPilot to call international numbers.

Getting there Messaging → Restriction Permission Lists → Long Distance 1 RPL or Long Distance 2 RPL

ATTENTION

Be cautious about the dialing codes you permit, and be careful about the features to which you apply this less secure list.

Applying RPLs

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.

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:

- Find the mailbox class members.
- Consider the calling requirements of the members and the restrictions needed for cost management and system security.
- For each mailbox class, determine which outdialing features are needed by mailbox owners in that class.
- For features mailbox owners do not need, ensure all dialing codes are restricted (digits 0–9 should be defined as the restriction codes).
- 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.
- 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”.
- 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).

Defining global restrictions and permissions for off-switch dialing

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**

Applying RPLs to thru-dialing services used by mailbox class members

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 → RPL settings**

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**

Chapter 8

Backing up and restoring CallPilot information

In this chapter

Overview

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

- Use backups to copy data to tape, disk or a remote disk drive.
- Schedule backups or perform them immediately.
- Restore archived information and full system backups.
- Monitor the status of a backup or restore operation.
- Review backup and restore history, and logs

Getting there: **In System → Backup/Restore**

Considerations and guidelines for backing up and restoring data

What 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 more often, especially if the data 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.
- 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.

How can the safety of backups be ensured?

Tape rotation scheme

Tape media that is used frequently eventually wears out and ceases to protect data properly. It is important to use multiple tapes in a rotation scheme to prevent the possible overwriting of good data with bad when performing tape backup or archives. Rotating several tapes extends individual tape life and enhances data resiliency.

Example of 3-tape rotation:

Week 1 use tape 1

Week 2 use tape 2

Week 3 use tape 3

Week 4 repeats cycle with tape 1

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.

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, selecting Backup overwrites 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.

Cleaning

- Include tape drive head cleaning in your regular backup routine
- Always clean the tape drive head after using a new data cartridge
- Always store the cleaning cartridge in a protective container

Storage

Do not store your backup tapes in the same location as your original data. Keep full backups at a separate, safe location. Ensure that only authorized personnel have full access to the sites and ensure that those responsible for maintaining backups fully understand their roles.

Store your backup media in an environment that meets the media manufacturer's storage requirements. Tape is sensitive to high temperatures (> 60 degrees Celsius/140 degrees Fahrenheit). Do not store the tapes in direct sunlight or near sources of excessive heat.

Defining backup devices and network destinations

These steps are not required if you use the tape drive for backup. The following steps are required to configure a remote backup disk:

1. Add a local user account to the remote file server.
2. Create and share a folder, and provide read/write access to the local user account
3. Add a new backup device using the shared folder.

4 Schedule a new backup using that device.

What you need before you can configure a remote backup disk:

- administrator access to the remote file server to configure a share for access by CallPilot
- the password of the local user account on the remote server

Types of backup devices

The Primary Server Tape is automatically listed 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 device. You cannot define a local disk as a backup device.

Predefined backup device

When the CallPilot server software is installed, only the Primary Server Tape is predefined as a backup device.

IPE system backups

All IPE systems are shipped with one drive. There are several system backup options for the server with one drive.

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 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 is replaced.

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 PDLs.
Prompt Archive	Backs up all custom prompts.
AppBuilder Archive	Backs up all custom applications.

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.

Backup type	Description
User Archive	Backs up all mailbox messages, personal information, greetings, personal verifications, and PDLs.
Prompt Archive	Backs up all custom prompts.
AppBuilder Archive	Backs up all custom applications.

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 NT/2000/XP/2003 remote file server. CallPilot does not support backups to local disks or remote disks on computers running Windows 95. For maximum security, restrict all access to the backup device to CallPilot Manager.

Configuring and scheduling backups

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 software problems (for example, file system corruption, registry corruption, or failed upgrades), undetected disk errors, double faults, human error, theft or damage caused by natural disasters
- create backups and archives that are used for migration to a different CallPilot platform.

Nortel recommends that you use the Backup and Restore option to schedule periodic backups (even on servers equipped with RAID). You can also define one-time server backups. Once defined, they run automatically at the scheduled time.

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

To avoid backup failure, do not schedule backups during the MMFS audit hour (3:00 a.m. to 4:00 a.m., server time). The speed with which backups are performed depends on system traffic and whether the backup device is local.

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

Archives

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

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

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 9*)
  - archive mailbox owners by last name in alphabetic segments (for example, a*, b*, . . . , z*)
- Prompt archives store all custom prompts recorded in a single language.

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

- AppBuilder archives store custom applications created using Application Configuring backups to the system backup tape.

Note: 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.

Note: Restoring a user archive from a TRP system to a 201i is not supported.

When to overwrite data and format the 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.

All backup tapes must be specially formatted for CallPilot server backup data. When you schedule a full system backup, selecting Backup overwrites 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, selecting Backup appends the new backup data to the existing contents of the tape.

Total Backup Elapsed Time table

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

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)
201i	SLR5	SLR5	350	2:55
702t	SLR32	SLR32	1000	1:56
702t	SLR50	SLR32	1000	1:56
702t	SLR50	SLR50	1000	1:28
703t	SLR60	SLR60	1200	0:25
1002rp	SLR50	SLR50	2400	1:42
1005r	SLR75	SLR75	2400	1:42

Performing an immediate backup to tape or disk

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.

Before you can perform an immediate full system backup

Ensure there is a backup listed in the schedule that is defined to meet your requirements 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.

Restoring from backups

Full system restore

Use the Backup and Restore Tool to restore a full system backup from a local tape or from a remote disk file server. A full system backup backs up all critical data, including messages and configuration information, on all drives. This includes all data that can be obtained by running the various archives. The OS or CallPilot software are not backed up.

Use the Backup and Restore Tool to perform a full system restore.

Restoring archives

Archives are backups of CallPilot multimedia files such as AppBuilder applications, personal user data (greetings, messages, personal verification, personal distribution lists), and customized voice prompts.

You can restore the following archive types:

- User archives store all CallPilot configuration information about mailboxes, mailbox owners, and administrators.
- Prompt archives store all custom prompts recorded in a single language.
- AppBuilder archives store custom applications created using Application Builder.

You can restore an archive while your system is online.

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, 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.

Monitoring the status of a backup or restore operation

When you have successfully started a backup or restore operation, CallPilot Manager shows the current status of the operation. If the backup or restore operation was scheduled for a specific date and time, select Status from the View list.

CallPilot Manager displays the 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.

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

Reviewing backup and restore history, and logs

When you need to view the details of a backup or restore operation, you can click View Backup History or View Restore History, or refer to the summary or detailed logs that are automatically created on the CallPilot server during a backup or restore operation.

Histories

You can use CallPilot Manager to view lists of histories for

- all system backups
- AppBuilder applications backups and restores
- custom system prompts backups and restores
- user (mailbox) data backups and restores

Backup and restore histories provide the following information:

- Archive Name
- Status
- Date
- Elapsed Time
- Type
- Total Size
- Device
- Summary Log
- Detailed Log

Logs

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

Logs can be viewed in the Backup History or Restore History screens. Click View In the Summary Log or Detailed Log column.

You can enter a value for the number of days to store history and log files in the History Options section.

Using the Backup and Restore Tool

You must use the Backup and Restore Tool to perform a full system restore. You cannot perform a full system restore from CallPilot Manager. Use CallPilot Manager for all backup and restore operations other than a full system restore.

Use the Backup and Restore Tool to:

- perform a backup
- query or add or delete a device
- perform a restore
- to diagnose a backup/restore
- display backup/restore history
- perform tape operations

Start the Backup and Restore Tool on the Windows Desktop.

Getting there: **Start → Programs → CallPilot → System Utilities → Backup and Restore Tool**

Chapter 9

Configuring addressing conventions and messaging service defaults

In this chapter

Specifying off-switch dialing prefixes

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

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

- 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).

Getting there: **Messaging → Dialing Information**

Handling mixed area or city codes

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

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

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	1 (Long distance)
Default Prefix	9 (Local)
Exchange Code list	555, 567, 579, 580, 597

Getting there: **Messaging → Dialing Information → Dialing Translations settings**

Defining address prefixes for both DTT and DTF

DTT and DTF addressing conventions

When you configure Delivery to Telephone (DTT) or Delivery to Fax (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

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 DTT 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 is not recorded because the greeting is still playing. Repeating the message makes it more likely that the entire message is 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 are able to listen to the content of the message.

Getting there Messaging → Outcalling Administration → Addressing settings

Enabling off-switch calls

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.

Connectivity restrictions

The Meridian 1 and Succession 1000 switches can capture an external CLID with an unknown format and then translate unknown dialing numbers into a default DN.

Getting there: **Messaging → Dialing Information → Dialing Defaults settings**

Changing messaging defaults

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
  - messages relating to network diagnostics (if messaging systems are networked)
  - 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 screen to configure the maximum delay for timed delivery, storage limits and warnings, and 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. Specify the number of minutes and seconds allowed for user mailboxes, and specify the percentage at which CallPilot generates a warning to delete voice items. Default: 1 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 is 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 2 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 1 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 length 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
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 screen 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 users of your system.

ATTENTION

Disable name dialing and name addressing features in countries where the keypads are not mapped to an alphabetical sequence that CallPilot recognizes.

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 screen.

The number of holidays inserted is limited to 60. Attempting to add a 61st holiday results in the following error message “The limit on number of holidays (60) has been reached.”

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**

Customizing system prompts

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.

CallPilot Manager displays a list of supplied system prompts for each installed language. Before you customize a prompt, listen to both the supplied system prompt and any customized prompt that is used to replace the supplied prompt.

When using your phoneset to listen to a system prompt, you must answer the phoneset within two or two-and-one-half ring cycles (for the Succession 1000). Before you can listen to a prompt, you must download the CallPilot Player.

To replace a supplied system prompt with a custom prompt, you must be able to provide the customized prompt. Before you can provide or edit a prompt, you must know the name and location of a suitable WAV file or have the CallPilot Player downloaded to your computer.

Note: A customized prompt is deleted when the user changes back to the system prompt.

Getting there: **Messaging → System Prompt Customization → Prompt ID**

Adding a corporate identity to system greetings

The administrator records a system greeting that precedes the personal greeting of all users during a call answering session. You can customize the content of seven system prompts. The seven prompts are displayed in the System Prompts Customization screen.

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.

Getting there: **Messaging → Messaging Management → System Greeting**

Dual Language Prompting

Dual Language Prompting provides system prompts in two different languages. This is intended for use in bilingual regions where a user may only be fluent in one of the two languages. Primary and Secondary languages can be selected among the installed languages. System prompts are then played in both Primary and Secondary languages one after the other.

Not all system prompts are played in both languages. The intent of this feature is to provide dual language prompts only for system prompts that are exposed to an unknown audience. Call Answer feature, for example, can be accessed by anyone that chooses to call a particular person that has a CallPilot mailbox. Similarly Remote Notification will send a message without knowing exactly who will be answering the call. Thus dual languages should be used. Prompts specific to a particular user are not played with dual languages. For example, the prompts played to a mailbox user after login do not need to be dual language. These prompts only need to be in the preferred language of the mailbox owner since only this user would be exposed to these prompts.

Getting there: **Messaging → Messaging Management → Installed Languages**

To enable this feature, a primary and secondary language must be selected, and the *Enable Dual Language Prompting* check box must be selected.

Configuring delivery to DNs not associated with CallPilot mailboxes

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 DTT and 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.

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. The DTT service 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 multi-delivery to fax service to specify the number of recipients to which an external fax message must be addressed before the fax is handled by the multi-delivery to fax service instead of the 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.

Task summary for setting up outcalling services

1 For 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 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 screen. Define for each condition how often and how many times the system tries to resend 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.

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

Chapter 10

Configuring CallPilot services

In this chapter

Voice messaging and call answering services

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.

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 others 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.

Outcalling services

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 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 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.

DTT replaces Meridian Mail delivery to non-user (DNU).

Delivery to fax

Enable 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.

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.

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

Remote notification

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

Enable 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 notified immediately whenever a message arrives at a help desk.

Addressing groups

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

- personal distribution lists (PDL)
- shared distribution lists (SDL)
- broadcast messages

Personal distribution lists

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 PDLs, each containing a maximum of 200 addresses. An address can be, for example, a local or remote mailbox, an SDL.

Shared distribution lists

SDLs are similar to PDLs, except that they are created by administrators. Maintaining a comprehensive list of SDLs optimizes your server capacity because it minimizes the need for mailbox owners to create their own PDLs and facilitates the use of broadcast messages.

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.

To be able to use SDLs, a mailbox owner must belong to a mailbox class that provides permission to use SDLs.

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

Benefits of maintaining SDLs

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 PDLs, 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.

Valid SDL members

You can include any CallPilot entity in an 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:

- RN targets
- non-users who require DTT

- SDL addresses

Getting there: **User → Shared Distribution Lists → Shared Distribution List Detail page → List contents settings**

Restrictions on SDL addresses

The following restrictions are placed on SDL addresses:

- An SDL cannot be assigned an address between 1 and 99. These are reserved for mailbox owners' 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**

Adding an SDL

Before you can create an SDL, you must know the SDL address that specifies the list.

Getting there: **User → Shared Distribution Lists → Add**

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.

Message notification options

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 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:

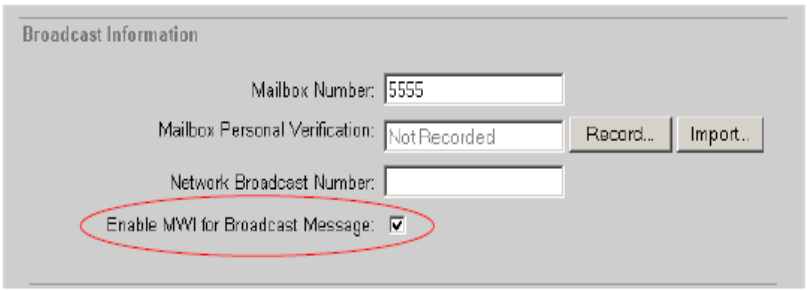
- On a digital phoneset, the MWI lights up.
- On an analog phone, the dial tone may be stuttered.
- On the desktop, the MWI is an icon in the form of a red phone. (If desktop messaging [a keycoded feature] is installed and enabled.)

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

Message Waiting Indicator (MWI) for Broadcast Messages

There is an option for turning off MWI for broadcast messages. By default MWI is turned on for broadcast messages.

Getting there: **CallPilot Manager → Messaging → Enable MWI for Broadcast Message** check box.



Configuration requirements

An 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 the 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.

- In CallPilot 4.0, multiple MWI DNs are supported. The system administrator can define up to eight MWI DNs for a mailbox. Whenever the message status changes, or the mailbox subscriber logs out, or during the night audit, all the MWIs at the DNs are updated. The message status also changes in the mailbox when the DNs are updated.
- You can configure the Multiple MWI feature through CallPilot Manager. In the CallPilot Manager (**Location → User → User Search → User Details**), you can input up to eight DNs for the MWI (MWI DN1 to MWI DN8). Each MWI DN has a check box for enabling and disabling, so that you can enable or disable an MWI DN individually. An MWI DN number can be changed only when it is enabled. When you save the page, all the data input for MWI DNs is written back to database, whether the MWI DN is enabled or not.
- In the Auto Admin page of CallPilot Manager, a group of new mailboxes can be added to the database in a single operation. CallPilot Manager adds eight MWI DNs to the choice list of the column selection drop-down box.
- When searching MWI DN with the Advanced Search in CallPilot Manager, the criteria for MWI DN covers all eight MWI DNs. As long as one of these eight MWI DNs matches the search criteria, this user can be returned by CallPilot Manager.
- MWI DNs are assigned by the administrator. Mailbox subscribers are not allowed to change their numbers. However, a mailbox subscriber can see these MWI DNs in the My CallPilot Features/Telephone Options page, and can enable or disable them individually. Only non-empty MWI DNs are displayed.

Remote notification of new or urgent messages

RN 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 RN capability
  - set default RN 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 RN 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 RN callback number.

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 (PDA), 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.

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).

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

- 99 PDLs, with 200 entries for each PDL
- maximum number of mailboxes:
  - IPE platform: 8000
  - tower and rackmount platforms: 20000

Message Forwarding Rule

The Message Forwarding Rule feature provides a way to configure CallPilot to automatically forward some or all CallPilot messages to an external e-mail address. This feature provides an easy way for users to access their CallPilot messages from third-party e-mail servers or to give other users access to their CallPilot messages. Messages received by CallPilot can automatically be forwarded to an address configured by the user from My CallPilot or by the system administrator from CallPilot Manager. This feature can also be used for message forwarding or for system-wide message archiving.

You must use CallPilot Manager to manage the Message Forwarding Rule feature.

You can provide and remove access to the Message Forwarding Rule feature within a Mailbox Class. You can also create, disable or alter an individual user's Message Forwarding Rule. Only the user can enable their rule however.

Configuring Message Forwarding Rule

Before you can configure the Message Forwarding Rule, you must first configure the Outgoing SMTP Mail/Proxy Server and the fully qualified domain name (FQDN).

Configuring the Server FQDN

1. In CallPilot Manager, navigate to **Messaging > Message Network Configuration.**
2. Select the Server name under the Local Server Maintenance window.
3. Click **Show Details**.
4. In the SMTP/VPIM section, enter the local server FQDN into Server FQDN.
5. Click **Save**.

Configuring CallPilot Manager Message Forwarding Rule

1. In CallPilot Manager, navigate to **USER > Mailbox Class** > click **Add**.
2. In the **Mailbox Class** dialog box, enter the class name.
3. In the Keycode Feature section, select the **Desktop and Web Messaging** check box.
4. In the Desktop and Web Messaging Configuration section, select the **Message Forwarding Rule** checkbox.
5. Click **Save**.
6. In CallPilot Manager, navigate to **User > Add User**. Enter the user details.

7. Click **Advance User Add**.
8. In the mailbox section of the drop-down list, select Mailbox Class.
9. In the Message Forwarding Rule section, click **Add**.
10. Select your Message to Forward from the drop-down list.
11. Choose either the E-mail or CallPilot address by clicking the appropriate button.
12. Select the **Mark original message as read** checkbox.
13. Click either **Forwarded by this service** or **Opened by recipient**, whichever is appropriate.

Notes: Opened by recipient functions if read receipt is supported by the recipient's E-mail service.

14. Select the appropriate button to Convert Voice Message to either VBK or WAV PCM.

Notes: VBK requires Nortel player.

15. Click **OK**.

Notes: MFR is not in effect until the user enables the rule from the desktop client.

To reduce unnecessary traffic on the CallPilot system, if the CallPilot sever detects an invalid e-mail address, the user's rule is disabled. The CallPilot server examines all NDNs received as a result of a Message Forwarding Rule. The Message Forwarding Rule is disabled if a message is unable to be delivered for any reason. Possible reasons include:

- incorrect address or address problem
- undiallable external DN
- bad destination mailbox address
- bad destination system address
- mailbox has moved

The user is notified at next login to My CallPilot. To permit the administrator to determine why the user's Message Forwarding Rule was disabled, a log is generated. Either the user or administrator is required to repair the e-mail address, and the user re-enables the rule from the Desktop or My CallPilot.

You also have the option to use the Message Forwarding Rule feature for system-wide message archiving instead of user-level Message Forwarding Rules. By enabling system wide archiving, you can set up a single e-mail address as the repository for all messages that enter the system. All messages that enter the system are automatically forwarded to the configured address. When message archiving is enabled, the Message Forwarding Rule check box in the Mailbox Class is unavailable. Users no longer see the Message Forwarding Rule link in My CallPilot or Desktop and all existing rules are disabled. It is the your responsibility to ensure the mailbox has sufficient storage space available to receive all incoming CallPilot messages and to back up these messages as needed.

Note: The Message Forwarding Rule feature (both archiving and message forwarding) applies to messages that arrive after the rule has been enabled. Existing messages are not processed by the Message Forwarding Rule or message archiving.

Preparing a Message to Forward or Archive

When a message arrives into CallPilot, the system first determines if the message is to be forwarded or archived. Before forwarding or archiving, the message contents are copied to a newly created message.

The message Body, To, CC, and From fields are reproduced in the new message. The date field displays the date when the message is deposited into the e-mail system, not the date the CallPilot server received the message. However, these two dates are virtually the same.

The Message Forwarding Rule feature redirects instead of forwarding the message to the specified address. The message appears as though it was sent from the originator, not the owner of the Message Forwarding Rule.

Message Subjects

The Subjects used for the Message Forwarding Rule are treated as follows:

- If the message has a subject, the original subject is used.
- If the message contains more than one voice, the duration is the total length of all voice messages.
- If the message contains more than one fax, the number of pages is the total pages of all faxes.
- If the **Mark original message as read when opened by recipient** option is selected, the Message ID is added to the beginning of the message subject. The message ID is followed by the originals subject.

Note: The subject is created the same way regardless of the order of the media types.

Mark Original Message as Read when Opened by Recipient

The feature makes use of the Read Receipt capability of the e-mail server the message was forwarded to. With this option enabled, a Read Receipt is requested to be returned to the CallPilot system when the forwarded message is Read. CallPilot recognizes the returned Read Receipt when either:

1. A MIME message with "Content-Type: multipart/report; report-type=disposition-notification" is received, AND, an "In-Reply-To:" or "References:" field is found containing the Message ID of the original message,

-or-

2. A MIME message with "Content-Type: text/plain" is received, AND, a subject field is found containing the string:

"[MsgId="the Message ID of the original message, and the string "]".

If CallPilot is able to extract the Message ID from an incoming Read Receipt, CallPilot marks the message with that Message ID as Read. If this was the only message in the user's mailbox that was Unread, the MWI light on the user's phone is turned off. If the message is already marked Read then no action will be taken.

Not all e-mail servers support Read Receipts. For example, at the time the document was written, Yahoo Mail and other popular e-mail servers did not support Read Receipts. It is up to the user to determine if their e-mail system supports Read Receipts.

To determine if the user's e-mail server supports Read Receipts, follow these steps:

1. Configure a CallPilot mailbox to forward to an account on the desired e-mail server.

2. Send a message to that mailbox. Verify that the MWI goes on at the corresponding phone (MWI DN).

3. Verify that the message is received at the e-mail account. (If possible, verify that a Read Receipt is requested.)

4. Read the message. (If possible, verify that a Read Receipt is sent out.)

5. Verify that the MWI light goes out on the phone (you may have to wait a minute or so).

Note: If the MWI goes out, this e-mail server currently supports Read Receipts.

Also, some systems give Read Receipts a lower priority than other messages, and Read Receipts may not be returned to the CallPilot system immediately.

Note: This feature is not supported by CallPilot systems, and the option will be disabled if a CallPilot address is selected.

Several recommended CallPilot SMTP proxy servers

- Microsoft Exchange 5.5
- Sun OS 5.8 (Solaris 8)
- Sun OS 5.7 (Solaris 7)
- Lotus Notes Domino Server 7.0 (If Inbound Relay Enforcement is not set)
- Novell GroupWise Server 6.5 (If SMTP Service is enabled)

Servers with known problems

Microsoft Exchange 6.5. When this server relays a message, it discards all tags for requesting read receipts and converts them to a single “Return-Receipt-To.” This tag is not supported by Microsoft Outlook. If an Exchange 6.5 e-mail server is used as the CallPilot SMTP proxy server, the Message Forwarding Rule “Opened by Recipient” option will not work for the users.

Troubleshooting

The administrator can troubleshoot this feature by asking the user to check their CallPilot mailbox for Read Receipts from the external e-mail server. If a Message ID is not found, the message is treated as a normal Read Receipt and deposited into the user's mailbox (without error). If the feature is working properly, there is no Read Receipts deposited into the user's mailbox; the Read Receipt is deleted when the associated message is marked as Read.

If the event code **54865 parsing error** is present in the Event log, a valid Read Receipt was received but a corresponding CallPilot message was not found. This is because the message had already been deleted.

The Event Log can be accessed in two ways:

1. Click the **Windows Start button → Programs → Administrative Tools → Event Viewer.**

2. Navigate to the CallPilot Manager: **System** tab → **Event Browser**.

If Read Receipts are not reliably returned or do not contain the required information, then the Message Forwarding Rule should be configured to either mark the message as being Read when the message is forwarded or clear the **Mark original message as Read** check box.

Automatic disabling of the user's Message Forwarding Rule

The user's Message Forwarding Rule will be disabled if the CallPilot server receives a Regular Non Delivery Notification (NDN) or Text NDN (English only, Exchange only) for any message forwarded by the rule. Nortel disables the rule as a way to warn the user that a problem occurred. The user will be informed that the rule was disabled the next time they log in to My CallPilot. They will need to resolve the problem and re-enable their rule from My CallPilot or Desktop.

An incoming message is considered a Regular NDN, and the user's rule is disabled, if the message meets both of the following criteria:

- The Regular NDN has a DR (Disaster Recovery) list containing the rule destination, or the DR list is empty.
- The Regular NDN contains the original message header.

An incoming message from an Exchange server is considered a Text NDN, and the user's rule is disabled, if the message meets all three of the following criteria:

- The Text NDN contains the original message header, including the MessageID of the original message.
- The Text NDN contains the field **X-MS-Embedded-Report**.
- The message subject does **not** start with "Read" or "Delivered."

Implications

1. Text NDNs received from non-Exchange servers are not interpreted as NDNs and the user's rule is not disabled.

2. Text NDNs received from non-English Exchange servers is not interpreted as NDNs and the user's rule is not be disabled.

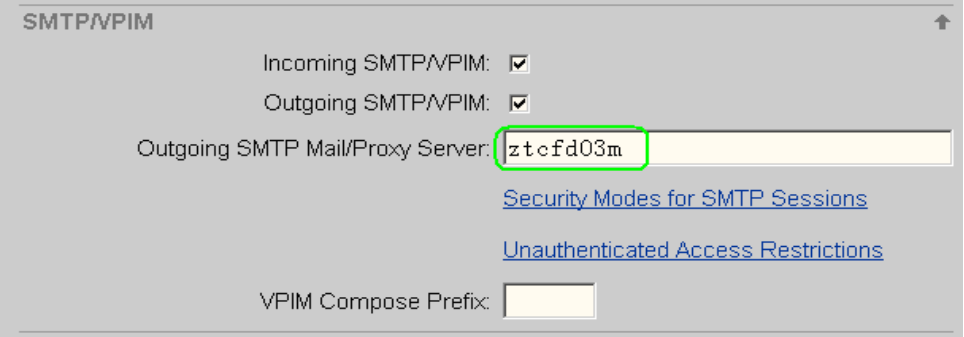
3. Some e-mail servers do not return NDNs. If no NDN is returned, the user's rule is not disabled.

Configuration Changes to Allow Outgoing Messages

SMTP Proxy is required for MTA to deliver the message, when auto-forwarding or archiving messages to the e-mail server.

To set SMTP Proxy Server:

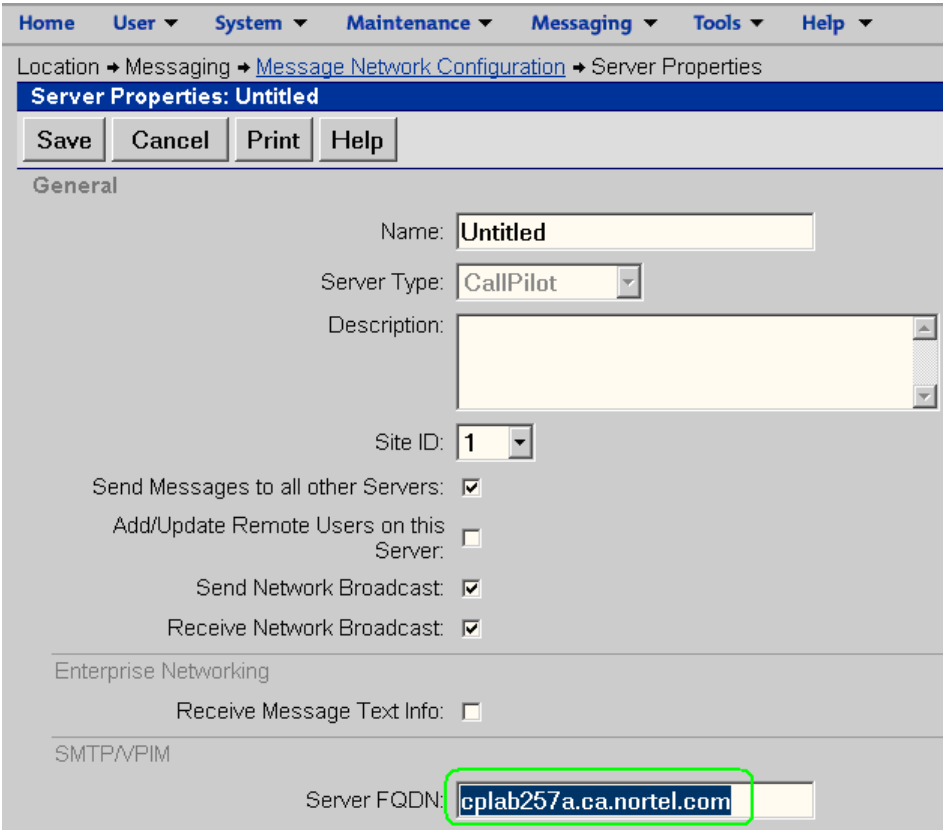
1. **CallPilot Manager →Messaging →Message Delivery Configuration**
2. Scroll to **SMTP/VPIM** section, input SMTP server name, FQDN or IP address **Outgoing SMTP Mail/Proxy Server**
3. Click **Save**



Set FQDN:

1. **CallPilot Manager →Messaging →Messaging Network Configuration**
2. Select Server name **Local Server Maintenance**
3. Click **Show Details**
4. Scroll to **SMTP/VPIM** section, input local server FQDN in **Server FQDN**

5. Click **Save**



Message Archiving

Archived messages are sent as Economy to reduce the impact on the system, regardless of the message being flagged Urgent, Normal, or, Economy.

If the CallPilot server detects an invalid address the system archiving is disabled. The user is notified at next login, requiring you to repair the error. Even if message archiving is disabled, addition of messages to the archiving queue continues. Message archiving continues when the problem has been resolved and message archiving is re-enabled.

When a message is archived, the audio format is not changed. Voice messages remain in VBK format.

For the Message Archiving feature, the Subject is treated the same way as stated previously for Message Forwarding Rules, but is extended to provide a way for the administrator to easily sort and identify archived messages. The To, From, Sender and CLID are displayed at the beginning of the Subject.

The subject of an archived message appears as follows: To: user-name [Mailbox#] From: sender-name [sender-CLID]: generated or original-subject (see table below).

The format outlined below is used to display the CLID and Sender's name:

CLID	**Sender's Name**	**Original Sender in the Subject**
Unknown	Unknown (but with system tag)	System
Unknown	Unknown	External
Known	Unknown	Unknown [CLID]
Known	Known	Sender-Name [CLID]

Note: The CallPilot subject field supports a maximum of 255 characters. If the original subject is longer than allowed, the remaining characters at the end of the subject are discarded.

Forwarding Restrictions

Message Forwarding Rule does not adhere to the Mailbox Class “Allow users to send voice messages to non-CallPilot recipients” option. Should the administrator want to prevent users from forwarding CallPilot messages off of the system, the Message Forwarding Rule can be disabled.

CallPilot addresses such as external phones, fax, and distribution lists are not supported by the Message Forwarding Rule. Only the following CallPilot address types are accepted:

- LOCAL - <local VPIM prefix><mailbox>@<local FQDN>
- NMS - <NMS location’s VPIM prefix><mailbox>@<local FQDN>
- Open VPIM - VPIM=<VPIM shortcut><mailbox>/<remote FDQN>@<local FQDN>
- Remote Mailbox - <remote location’s VPIM prefix><mailbox>@<local FQDN>

If a recipient address is not resolved by the Address Module, the message is not delivered. You or the user must check that the recipient address is correct. Event 55091 is sent to the event log.

CallPilot distribution lists are not supported with this feature. If a message is addressed to a CallPilot distribution list, event 55092 is sent to the event log and the user interface does not allow the address to be saved. Note that e-mail distribution lists are supported. An e-mail distribution list can be entered as an e-mail address in the Message Forwarding Rule.

If a message is not forwarded to the same user mailbox that owns the Message Forwarding Rule (original sender). Event 55092 is sent to the event log.

If the Message Forwarding Rule fails due to an LDAP search error, the newly arrived message cannot be forwarded or archived. Ensure the LDAP server is running. Event 55093 is sent to the event log. If this persists contact Customer Service Representative (CSR).

A message for forwarding failed to be composed or deposited to MTA, preventing the message from being archived or forwarded. Event 55094 is sent to the event log. Ensure the MAS Multimedia is running. If the problem persists, contact your Customer Service Representative (CSR).

A single message cannot be forwarded more than two times. For example if user A forwards to user B, user B forwards to C, and user C forwards to user D, the Notification Server does not forward the message to user D. Event 55095 is sent to event log.

Feature Limitations

The following is a list of feature limitations for the Message Forwarding Rule:

- A rule is limited to one e-mail or CallPilot address.
- There is a maximum one rule per mailbox.
- CallPilot distribution lists are not supported.
- Synchronization between e-mail and CallPilot server is not supported.
- Messages must be deleted from both e-mail and CallPilot accounts, however, CallPilot can be configured to AutoDelete messages after they are read.
- Partial synchronization is supported. The user must mark CallPilot messages as “read” when the message is opened from e-mail server (e-mail server must support Read Receipts).
- Fowarding is not based on importance (Urgent, Normal, Economy), sensitivity (Private or Normal), time, date, sender, or subject, and so on.
- Voice messages cannot be played over telset from a computer once they are converted to WAV.
- Microsoft Outlook, Lotus Notes, and Novell GroupWise Desktop Messaging users that activate a rule see two occurrences of the same message, once in CallPilot view and again in their e-mail inbox.
- The scheduler attempts to resend a message three times an hour for a maximum of 48 hours.

Note: You can prevent users from forwarding CallPilot messages outside the system by disabling the Message Forwarding Rule feature.

- The Message Forwarding Rule configuration page only provides simple address validation and checks for CallPilot addresses.
- If an invalid address is entered, an NDM is sent to the originator, and the Message Forwarding Rule is disabled. The user must check and correct the address, and enable the Message Forwarding Rule.

Notes:

1. The interface does not prevent the user from configuring a rule to forward fax messages to a user who has no fax capability, or CallPilot messages to an invalid CallPilot mailbox.
2. In order to enable or disable Message Forwarding Rule on the desktop client interface use the account information in the users Address Book advance section, not an anonymous log on.
3. Message Forwarding Rule is ignored if **Allow user to send messages to non-CallPilot recipients** is checked. The Message Forwarding Rule overrides this selection and messages are forwarded. You can manually set these features if **Allow user to send messages to non-CallPilot recipients** is unchecked, do not set the Message Forwarding Rule for the user.

Speech activated messaging

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).

Addressing capabilities

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

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 DN

- 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 RNcallback DN.

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

In CallPilot 4.0, desktop users can insert authorization and access codes within the fax Directory Numbers (DNs). CallPilot 4.0 is enhanced to permit timed pauses and number-sign digits within the DN addresses.

The following components support the pause architecture:

- CallPilot Manager
- Desktop Client
- Deb Messaging
- My CallPilot
  - Support for DN addresses with pause or number-sign digits
- Address Module
  - Validating DN addresses with pause or number-sign digits
- Telset Application services
  - Performing outgoing calls with pause or number-sign digits
- TAPI Translation Layer
  - Conversion of commas or asterisks to the appropriate switch representation

The following two-digit characters are available:

- *(asterisk, 2-second pause)
- , (comma, 2-second pause)
- P (upper- or lowercase letter P, 2-second pause)
- # (number-sign, for supporting authorization codes and access codes that follow a PSTN)

Pause support is available for:

- Telephone addresses

- Fax addresses
- Mailbox Revert DN (asterisk and commas are permitted, but number-sign is not permitted)
- Mailbox Default Printing DN
- Mailbox Remote Notification DN

Asterisk, commas, or number-sign digits are available in the following applications:

- CallPilot Manager
- My CallPilot RN target DN setup

The letter P (upper- or lowercase) or number-sign digits are available in the following applications:

- Desktop Client
- Web Messaging

Note: The Telset interface does not support entering any pause or number-sign digits.

A comma (instead of a p or P) is required if adding a pause from an IMAP client.

The 2-second timed pause is a system-wide (administrator readable only) default. It is viewable using:

- **CallPilot Manager → Messaging → Message Delivery Configuration Menu → Remote Contact:AMIS/Enterprise**

Outcalling details

- Outcalling includes Delivery to Telephone (DTT), Delivery to Fax (DTF), and Remote Notification (RN) services.
- Pause or number-sign digits are not supported for internal DNs.
- Digits following the first number-sign are out-pulsed separately. Any asterisk digits are interpreted as the digit asterisk and not a 2-second pause.

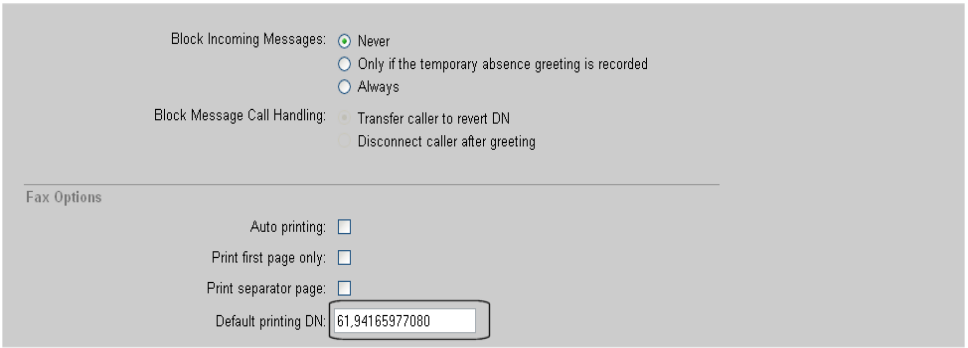
- Attendant DN can use only commas or asterisks and cannot use number-sign digits.
- For Analog and DTI trunks, the end-to-end speech path from the CallPilot to the far-end station switch must be established for the pause character to function correctly.

  Note: ISDN trunks do not support the pause architecture.

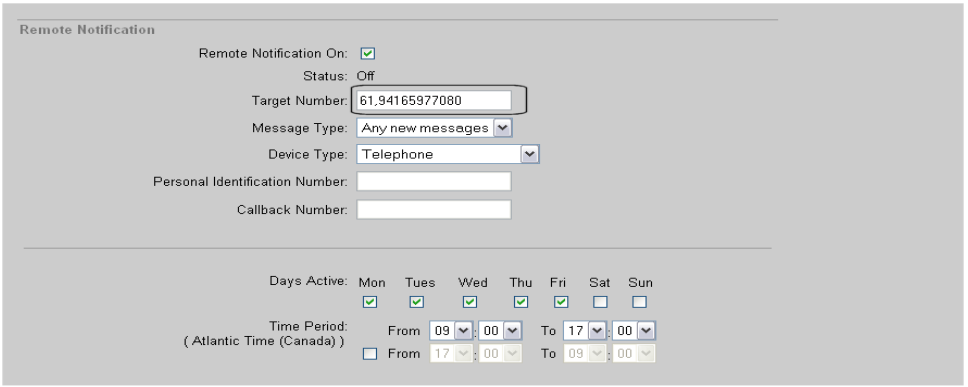
The following figure shows an example of a pause digit within the Mailbox Attendant DN:

61 → External Trunk Access , → 2-second pause for second dial tone
9416597080 → External Attendant DN

The following figure shows an example of a pause digit within the Mailbox Default Printing (DN):

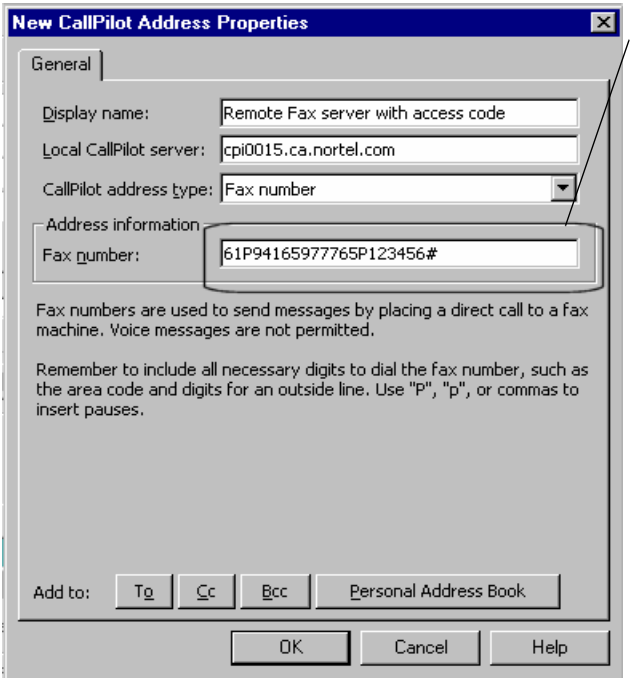


The following figure shows an example of a pause digit within the Mailbox RN Target DN:



Composing using CallPilot Desktop

The following figure shows an example of composing using CallPilot Desktop - Addressing to a remote Fax service using Authentication Codes.



61 → external Analog/DTI trunk access,

P → 2-second pause for second dial tone,

94165977765 → Remote Fax service,

→ for ISDN-style trunks

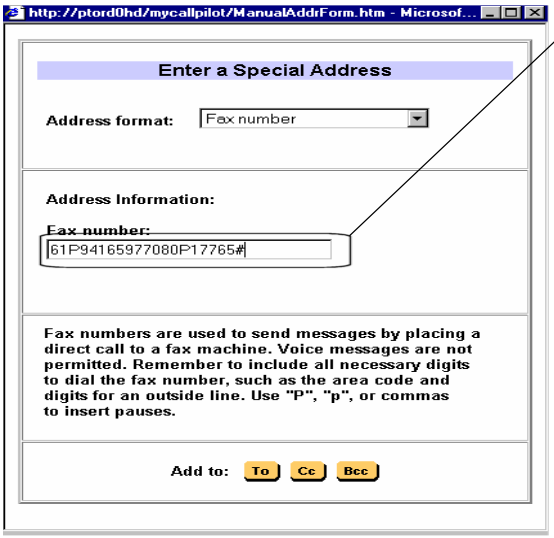
P → 2-second pause while remote connection is established,

123456 → Remote Fax Service Access code,

→ Access code terminator

Composing using Web Messaging

The following figure shows an example of composing using Web Messaging - Addressing to remote Fax service using Authentication Codes.



61 → external Analog/DTI trunk access,

P → 2-second pause for second dial tone,

94165977080 → Remote Fax service,

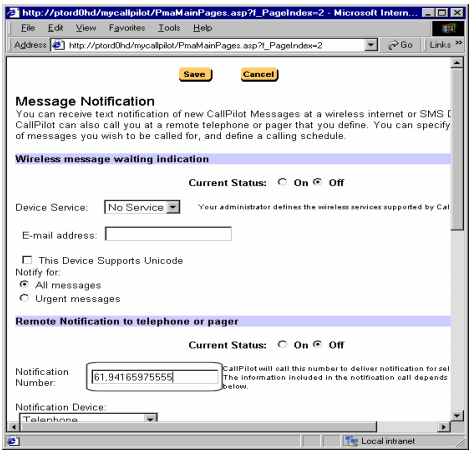
→ for ISDN-style trunks

P → 2-second pause while remote connection is established,

17765 → Remote Fax Service Access code,

→ Access code terminator

The following figure shows an example of using My CallPilot to configure RN - adding pause characters within RN using My CallPilot.



Pause Support Troubleshooting

In addition to any event logs, the following notifications are available.

Service	Notification Type
Telephone DN	NDN
Fax DN	NDN
Mailbox Revert DN (number-sign is not permitted, only asterisk or commas)	N/A
Mailbox Default Printing DN	N/A
Mailbox Remote Notification DN	Mailbox summary after login (Telset only)

Troubleshooting

Problem: Your message did not reach some or all of the intended recipients.

Symptom:

- Subject: (no subject)
- Date: Mon, 28 Jan 2002 17:26:21 -0500 (Eastern Standard Time)
- The following recipient(s) could not be reached:
- "Unknown" <VOICE=99,,99999999@cpi0005.ca.nortel.com>
- Reason: The external telephone number used in addressing the message could not be dialed.

1 Check the NDN reason explanation (if available).

2 Attempt manual dialing of the number with estimated pause timings

3 Verify that DNs without pause or number-sign digits are OK.

4 If the Telset Application service did not start, check the address format on the server-side.

5 Check whether the Telset Application service was involved. i.e. Reproduce the problem and check whether the appropriate application service started.

6 If the Telset service started then a SLEE trace may be required for further analysis.

7 Remote Notification, Default Fax DN Attendant Transfer issues require Telset application investigation (SLEE trace).

8 If you are using ISDN and further analysis is needed the following information is required:

- M1: D-Channel (Monitor level 2) and ELAN traces
- CallPilot: AML, and SLEE traces

9 If you are using ISDN, ensure the speech path is established before the pause characters are sent.

10 Using speed dial, verify dialling the number with all the appropriate pause character and number-sign digits. If the call cannot be completed using speed dial, it will not work using CallPilot.

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.

Service directory numbers

To make a service or application available to callers, you must add a unique 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.

In addition to providing a unique DN for each CallPilot service, the SDN configuration also determines certain aspects of the service 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 DN

Multiple SDNs for a single service

Create more than one 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 SDNs are automatically created by the system during installation. You cannot

- create or delete an outbound SDN
- rename an outbound SDN
- change the actual SDN (This number is specific to each service and is automatically assigned.)
- modify the session profile or callback handling properties

Adding inbound Service Directory Numbers (SDNs)

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. You must know the controlled DN or phantom DN configured on the switch for the service you are adding.

The Maximum number of SDNs that you can add for each server is:

- 201i - 500
- 703t - 2500
- 1002rp - 2500
- 1005r - 2500

Note: You cannot add or delete an outbound SDN.

Getting there: **System → Service Directory Number**

Configuring a session profile for messaging services

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 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

Broadcast capabilities

Use the Messaging Management screen to define the numbers that mailbox owners must specify when they compose broadcast messages. 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). A local broadcast is a voice message that is delivered to all of the users on the local system. A location broadcast is a message that is sent to all users at a specific remote site or switch location in the messaging network.
- both local broadcast and network broadcast (includes network location broadcast) capability. 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.

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.

Note: The Mailbox number field in **Messaging Management - Broadcast Information** must not be left blank. The **Network Broadcast Number** is blank by default.

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.

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 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.

Getting there: **Messaging → Messaging Management → Broadcast Information settings**

Fax (multimedia) messaging

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 through 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.

Configuring a fax service

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**

Configuring callback handling for a fax service

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 DN. 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 are 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**

Configuring a custom cover page for a fax service

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**

Configuring 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

Logon by means of 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

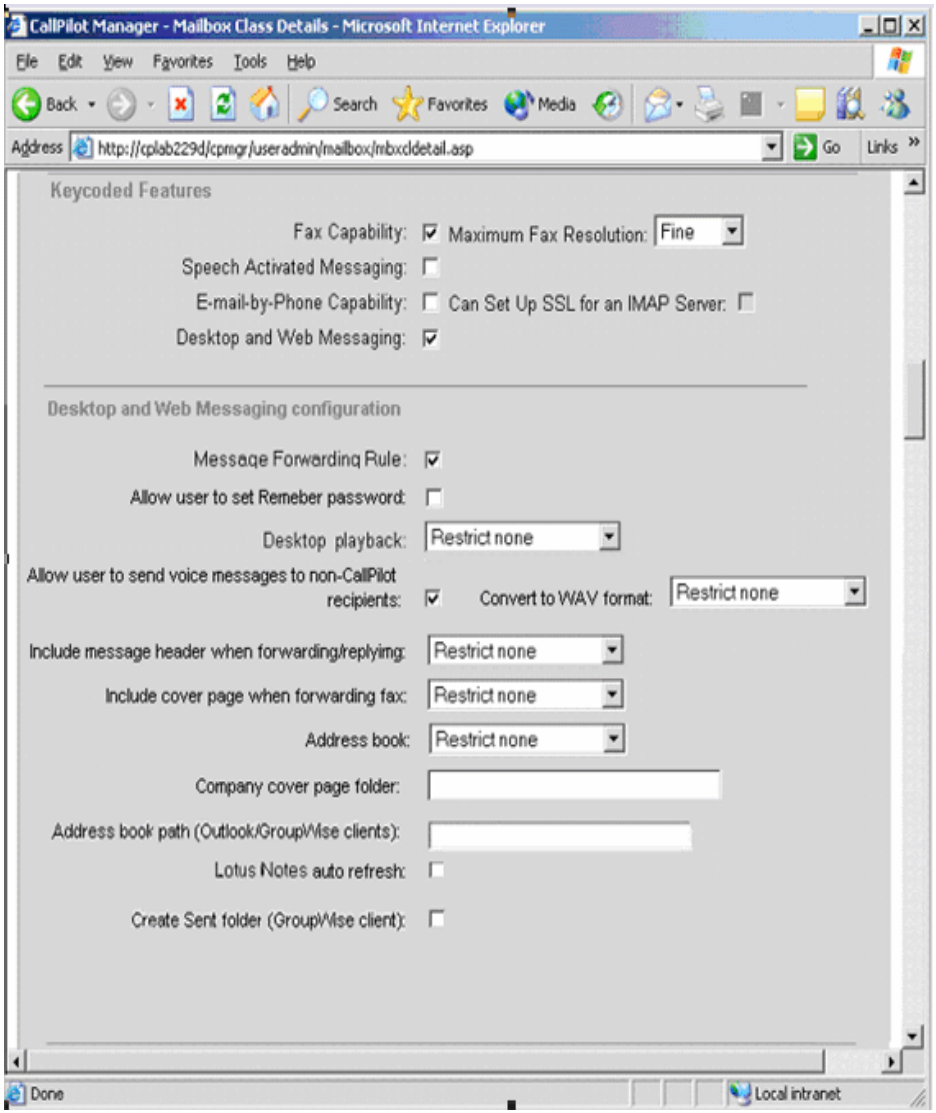
No special installation or switch configuration is required.

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.

Configure alternate phoneset interfaces to support new CallPilot mailbox owners who are accustomed to using another messaging system. CallPilot supports the 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 overrides 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

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 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 of alternate phoneset interfaces

- no extended message header
- provide the short message header option only.
- no on the phone notification prompt
- no administrative prompts such as those for recording the system greeting or another mailbox owner's personal verification.
- no commands to create or print fax messages
- no RN or remote text notification administration prompts and commands
- mailbox owners must use the CallPilot UI to configure notification settings
- no prompts or commands for maintenance of PDLs
- invalid PDL entries are not auto-deleted
- DTMF Confirmation Required for DTT prompt
- no CallPilot economy delivery option
- speech activated messaging provides only CallPilot prompts and commands
- provide prompts and commands for auto printing fax messages and for printing a fax separator page, but not for administering those functions
- callers who access a mailbox by name dialing do not receive prompts provided by alternate phoneset interfaces
- prompt terminology differences among the phoneset interfaces
- revert DN works only if the caller presses zero before the end of the mailbox owner's recorded greeting

Configuration tasks

The following configuration tasks allow mailbox owners to be transitioned to the CallPilot phoneset interface without requiring new logon DNs.

- Ensure that the mailbox class setting determines the phoneset interface for all mailbox callers.
- 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.
- 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.
- Apply the appropriate new mailbox class to each existing mailbox owner who prefers the alternate phoneset interface.

Ensuring access to features exclusive to CallPilot

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.

Ensuring use of the preferred phoneset interface

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 is presented.

Getting there: **System → Service Directory Number → Service Directory Number page → Session Profile**

Making the alternate phoneset interface available to users

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

You need the controlled DN or phantom DN configured on the switch for this service.

Getting there: **System → Service Directory Number → Service Directory Number Details page → General**

Configuring Symposium Voice Services support

Symposium Voice Services support

- provides unified messaging to Symposium Call Center personnel
- allows the 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 Email-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

- The switch informs the Symposium Call Center server that a call has arrived at the ACD queue.
- The Symposium Call Center server routes the call to the ACD queues.
- 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.
- 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 DNs from the switch by means of the Application Module Link (AML) and voice port channels from CallPilot by means of 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 DNs 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 AML connection.

ATTENTION

AML allows resources to be associated with one AML connection only. This means that the CallPilot AML connection with the switch cannot be used to control voice channels already acquired by Symposium.

- The switch communicates with CallPilot through 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 or later, 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 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:

- Each voice port DN configured on the switch and the Symposium Call Center server are also be configured on the CallPilot server.
- The ACD queue configured on the switch for ACCESS channels is configured as the Symposium Voice Services ACD queue in the CallPilot SDN table.
- The ACD queue 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.

ATTENTION

CallPilot requires at least one port to be configured as multimedia or voice messaging. If all ports are configured as IVR in the Configuration Wizard, the ELAN is not established successfully when the system is rebooted. CallPilot requires at least one multimedia channel for its own use.

Configuration tasks

- On the switch:
  - Configure separate embedded LAN (ELAN) and value added server (VAS) IDs for Symposium Call Center and CallPilot.
  - Configure an ACD queue for the ACCESS agent and an ACD queue for the IVR agent.
  - Configure each ACCESS and IVR port.
- 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 the CallPilot channel allocation.

  - Use CallPilot Manager to add service DNs for Symposium Voice Services and the Application Builder announcement or voice menu.

Troubleshooting Symposium Voice Services support

If the following events occur, you need to troubleshoot the Symposium Voice Services support:

- The Event Browser displays a Meridian link TSP or ACCESS link event.
- Mailbox owners 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 ACD queue for ACCESS channels configured as the Symposium Voice Services SDN?
  - Is the ACD queue for IVR channels configured as the Symposium Voice Services support announcement or voice menu SDN?
  - Does the Class ID configured through 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 ACD queue for ACCESS channels configured so that IVR=YES and ALOG=YES?

- Is the ACD queue 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?

Dynamic channel allocations

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 SDN are not used. Instead, the channel allocations assigned to the DTF SDN are used, because the DTF 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

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 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.

This section provides several examples of how channels might be re-allocated temporarily to accommodate a typical 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 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 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.

Getting there: **System → Service Directory Number → SDN Details**

Email-by-Phone with CallPilot Manager

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.

The steps for configuring the Email-by-Phone feature are as follows:

- Configure the external e-mail server
  CallPilot Manager → Messaging → External E-mail Servers.
- Configure the user's class of service
  CallPilot Manager → Messaging → User → Mailbox Classes.
- Configure the user's e-mail account
  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.
  CallPilot Manager → Messaging → User → User Search.

To be able to execute the configuration procedures, you must be logged in to CallPilot Manager.

Email-by-Phone with My CallPilot

Once the administrator has 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.

The Email-by-Phone feature can be used only if the external e-mail server supports the IMAP r4 protocol.

Networking solutions

CallPilot supports the following types of networking solutions:

- VPIM networking
- Enterprise networking
- AMIS networking

After you purchase the networking keycodes, the networking solutions are available for your site. During installation of CallPilot, you 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 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.

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

Refer to the *Network Planning Guide* (555-7101-102) for detailed information on selecting the type of networking appropriate for your site.

Application Builder

Application Builder is a graphical software program that allows the you 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. Refer to the *Application Builder Guide* (555-7101-325.)

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.

Desktop messaging and My CallPilot

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.

Centralized Control of Desktop Options

The Centralized Control of Desktop Options feature permits you to control the features of the CallPilot Desktop Messaging client. This is achieved through the new Class of Service settings on the CallPilot server.

CallPilot 4.0 adds the following new Class of Service settings:

- Require SSL
- Allow user to set Remember password
- Allow user to send voice messages to non-CallPilot recipients
- Convert to WAV format
- Include message header when forwarding/replying
- Include cover page when forwarding fax
- Address book
- Company cover page folder
- Address book path (Outlook or GroupWise clients only)
- Lotus Notes auto refresh
- Create Sent folder (GroupWise client)

Changes made to Centralized Control of the Desktop options are not detected while the desktop clients are running. End-users must close the desktop client and log on again to enable the latest changes. You can toggle the settings in CallPilot Desktop Messaging Class of Service.

Chapter 11

Monitoring the CallPilot server and resources

In this chapter

Viewing the performance of CallPilot server

To view the performance of CallPilot server, click Performance Monitor on the System menu. 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 fixed disks.

Finding information about the CallPilot server

You may need Server Settings information when you communicate with product support personnel. To view CallPilot server settings, click Server Settings on the System menu. Use the Server Settings screen 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, Email-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 screen to display a list.

Finding information about the connected switch

Use the Server Settings screen to display switch information such as:

- the switch type (for example Meridian 1 or Succession 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 screen to display serial port configuration information such as:

- port type
- baud rate
- data bits
- parity
- stop bits
- flow control

Running system reports

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 OMs that you can review, monitor, and evaluate with CallPilot Reporter. CallPilot collects OM data on the OM server in 1–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.

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.

Monitoring call channels

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, identify which call channels are not functioning, and identify the physical location of a channel by its icon position on the Channel Monitor screen. Channel Monitor also displays a channel directory number (DN) and position (Label) in a pop-up when you move the mouse cursor over the channel 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 is 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.

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 changes 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

Monitoring multimedia channels

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 the physical location of a call channel by its position on the Multimedia Monitor screen
- 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.

Multimedia Monitor also displays a channel (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 is 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 screen 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 changes 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

Monitoring disk space

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 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 DNs, and OMs, which are raw data about the system.

Nightly audit

Each night, the CallPilot server performs an audit that cleans up expired files in the MMFS 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.

Monitoring Nortel directory disk space

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 SPM.

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

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 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, particularly if you must add new users to the system.

General methods to monitor disk space

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.

The SPM provides detailed information on the disk space available on the system.

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* (555-7101-310).

Administrative actions

- Decrease the amount of time that the system retains messages before they expire if you discover that the MMFS is getting full.
- 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).
- 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 (OM retention).

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.

Monitoring the database

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 do 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. 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.

Events

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

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

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

Event severity

- 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 driver events, appear as event code 40592 in the Event Browser and in the system log in the Windows 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 Event Viewer. This is an information event, so it does not appear in the Alarm Monitor.

Using the Event Browser versus the Alarm Monitor

The Event Browser and Alarm Monitor both show events that occur on the server. These programs provide many common features for viewing events. The following table lists each feature and the program that offers the feature.

Event Browser versus Alarm Monitor feature matrix

Feature	Event Browser	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
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 Simple Network Management Protocol (SNMP) filtering criteria	No	Yes

a.Events can be customized in the Event Browser. However, these changes also affect the generated alarms.

The Event Browser performs 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 Alarm Monitor 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.

Changing the event log size

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 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 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.

Windows Event Viewer

The Windows 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.

Use the Windows 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)

Viewing events in the Event Browser

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.

Getting there: **In System → Event Browser**

Filtering events in the Event Browser

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

Saving and printing a list of events from the Event Browser

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.

Throttling events (reducing the frequency of events)

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 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.

Filtering by changing event properties

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.

Viewing alarms in the Alarm Monitor

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 generate an event several times, with the same Object ID and the same Instance, then the event appears only once in the Alarm Monitor.
- If you customize events in the Event Browser, those changes do affect the Alarm Monitor. For example, if an event severity is changed from minor to information, the event does not generate an alarm. Also, if an event severity is changed from minor to major, the severity of the generated alarm is 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.

Getting there: **In System → Alarm Monitor**

Filtering SNMP traps

Access the SNMP Settings screen from the Alarm Monitor to determine which SNMP traps, based on severity, are sent out from CallPilot.

Clearing active alarms

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.

Configuring SNMP on the CallPilot server

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:

1. Configuring SNMP on the CallPilot server so that the traps are directed to an NMS.
2. Configuring the NMS so that it can receive the CallPilot SNMP traps.

Configuring SNMP Agent Information

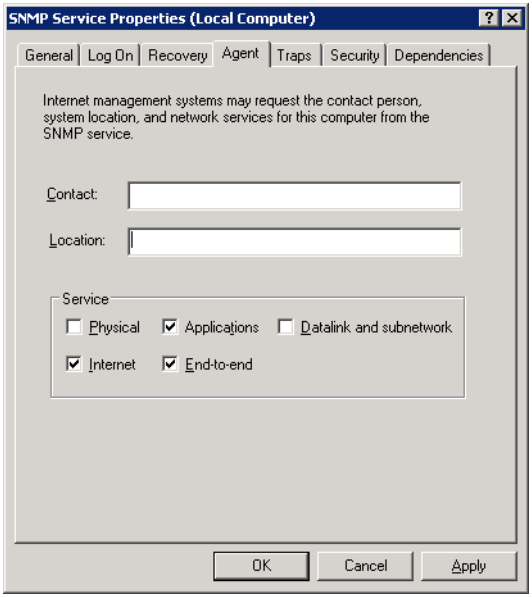
1 Click Start > Settings > Control Panel > Administrative Tools, and then click Computer Management.

2 In the console tree, expand Services and Applications, and then click Services.

3 In the right pane, double-click SNMP Service.

4 If the SNMP service status is “started”, stop the service by clicking on the “stop” button.

5 Click the Agent tab.



6 Type the name of the user or administrator of the computer in the Contact box, and then type the physical location of the computer or contact in the Location box.

7 Under Service, click to select the check boxes next to the services that are provided by your computer. Service options are:

- Physical: Specifies whether the computer manages physical devices, such as a hard disk partition.
- Applications: Specifies whether the computer uses any programs that send data by using TCP/IP.
- Datalink and subnetwork: Specifies whether this computer manages a TCP/IP subnetwork or datalink, such as a bridge.
- Internet: Specifies whether this computer acts as an IP gateway (router).
- End-to-end: Specifies whether this computer acts as an IP host.

8 Click **OK**.

Configuring SNMP communities and traps

1. Click Start > Control Panel > Administrative Tools > Computer Management.
2. In the console tree, expand Services and Applications, and then click Services.
3. In the right pane, double-click SNMP Service.
4. Click the Traps tab.
5. In the Community name box, type the case-sensitive community name to which this computer will send trap messages, and then click Add to list.
6. Under Trap destinations, click Add.
7. In the Host name, IP or IPX address box, type the name, IP or IPX address of the Network Management host, and then click Add.

   Result: The host name or address appears in the Trap destinations list.
8. Repeat steps 5 through 7 to add the communities and trap destinations that you want.
9. In the general tab, click the start button to start the service.
10. Click **OK**.

Chapter 12

Voice Messaging—Verbose Help User Interface

In this chapter

Overview

Voice Messaging—Verbose Help User Interface is an enhanced standard CallPilot User Interface and provides expanded delay prompting during message retrieval and status sessions. All commands that are acceptable for CallPilot User Interface (UI) are acceptable for Voice Messaging—Verbose Help User Interface.

Voice Messaging—Verbose Help User Interface

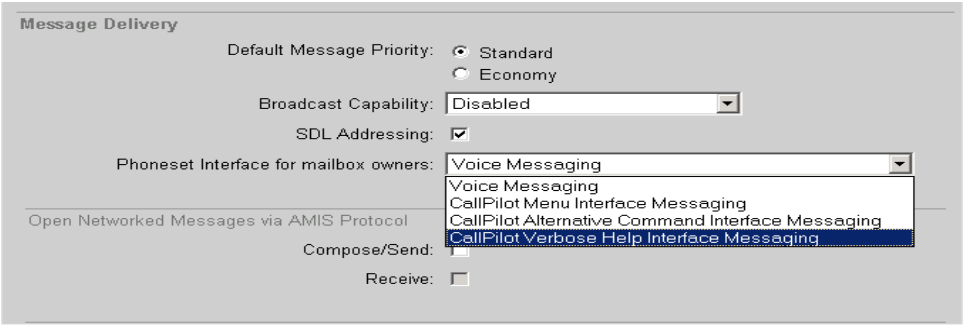
Voice Messaging—Verbose Help User Interface is an enhanced CallPilot User Interface (UI) that is designed to help users become familiar with the functions available in the voice messaging environment. Voice Messaging - Verbose Help User Interface helps users navigate more effectively by presenting a more detailed set of help prompts.

Voice Messaging—Verbose Help User Interface provides users with more detailed explanations when users want to compose, play, reply, forward, or delete a message. In addition to describing scenarios in context, Voice Messaging—Verbose Help User Interface also provides users with more options in the delay prompts than are available with the standard Meridian Mail User Interface (MMUI). All commands that are acceptable for CallPilot UI are acceptable for Voice Messaging—Verbose Help User Interface.

New for Voice Messaging—Verbose Help User Interface

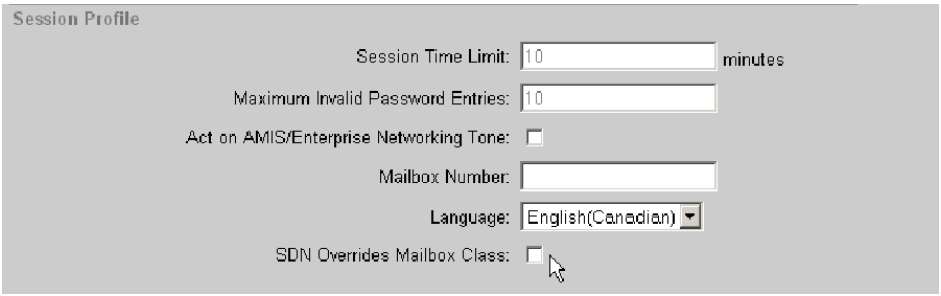
The Voice Messaging—Verbose Help User Interface, a new control item is added to the Mailbox Class properties.

User→Mailbox Classes (Select Mailbox Class)



This control item allows creating new types of mailbox classes for users who want expanded prompts for the various message contexts.

Note: When you select CallPilot Verbose Help Interface Messaging, you must ensure that the Voice Messaging SDN is configured properly. When you select **Service Directory Number →SDN Details**, go to the Session Profile area. In the Session Profile area, you must clear the **SDN Overrides Mailbox Class** check box for Verbose Help User Interface to work.



Chapter 13

Preventive maintenance guidelines

In this chapter

CallPilot preventive maintenance guidelines

1 Maintain a log book.

Maintain a log book where any maintenance activity performed should be recorded diligently. This can be extremely useful in diagnosing problems. The log book 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 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 server should have a name associated with the activity recorded in the log book as mentioned in item 1.

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 7, “Backing up and restoring CallPilot information”

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.

6 Use CallPilot Reporter.

Reporter is another excellent tool to understand the usage of CallPilot. It is useful in understanding the heavy users, the heavy usage times and other patterns.

Refer to the *CallPilot Reporter Guide* (555-7101-310).

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.

8 Monitor MMFS volumes.

Verify using CallPilot Reporter that the MMFS usage is below 90 percent on all MMFS volumes. If any volume is above 90 percent then the mailboxes may have to be rebalanced to other volumes.

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.

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.

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.

12 Use of pop up blocking software

If pop up blocking software is installed and enabled, pop up dialog boxes in CallPilot Manager and My CallPilot are prevented from functioning. Use of this software is not recommended.

Index

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Administrator's Guide

CallPilot
Release 4.0

Document Number: 555-7101-301

Document Version: Standard 1.18

April 2007

All Rights Reserved.

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

*Nortel Networks, the Nortel Networks logo, and the Globemark are trademarks of Nortel Networks.

*Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

NORTEL