555-7101-507

CallPilot

Networking Enhancements Guide

Product release 2.0 Standard 1.0 September 2002

NORTEL NETWORKS™

CallPilot

Networking Enhancements Guide

Publication number:	555-7101-507
Product release:	2.0
Document release:	Standard 1.0
Date:	September 2002

Publication history

September 2002

Standard 1.0 of the CallPilot 2.0 *Networking Enhancements Guide* is released for CallPilot 2.0 general availability.

Contents

Chapter 1

About this guide

In this chapter

What's new in networking

Introduction

The *Networking Enhancements Guide* provides a brief description of the features and capabilities that have been added to the networking solutions for CallPilot 2.0.

SMTP authentication

You can secure your messaging network by authenticating SMTP connections between the following:

- desktop or web messaging users and the CallPilot server
- the CallPilot server and voice messaging systems at remote sites (applicable to VPIM Networking only)

SMTP authentication prevents hackers from connecting to your CallPilot server, thereby reducing the risk of junk e-mail proliferation or denial of service.

Note: This guide focuses on SMTP authentication between voice messaging systems only. For information about SMTP authentication and desktop or web messaging users, refer to the CallPilot Manager online Help and the following documents:

- *Desktop Messaging and My CallPilot Installation Guide* (NTP 555-7101-505)
- *Desktop Messaging and My CallPilot Administration Guide* (NTP 555-7101-503)

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 page in CallPilot Manager (manual monitoring)

  You can manually monitor activity based on the following:

  - host name 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

Encryption

You can guarantee the privacy of messages transmitted over the network by encrypting connections between the following:

- desktop or web messaging users and the CallPilot server
- the CallPilot server and voice messaging systems at remote sites (applicable to VPIM Networking only)

Encryption prevents others from listening to or viewing the contents of messages while they are in transit.

Note: This guide focuses on encryption between voice messaging systems only. For information about encryption and desktop or web messaging users, refer to the CallPilot Manager online Help and the following documents:

- *Desktop Messaging and My CallPilot Installation Guide* (NTP 555-7101-505)

- *Desktop Messaging and My CallPilot Administration Guide* (NTP 555-7101-503)

Network and location-specific broadcast

Mailbox owners can send broadcast messages to other users

- at the local site (local broadcast)
- at a specific remote site (location broadcast)
- a specific Network Message Service (NMS) location at the local or remote site (location broadcast)
- all sites and locations (network broadcast)

Prior to CallPilot 2.0, mailbox owners could only send broadcast messages to mailbox owners at the local site (local broadcast).

Note: All NMS locations associated with the local site also received the local broadcast.

Names Across the Network

Names Across the Network (NAN) is a feature that allows the spoken names of message senders to be reproduced at recipient sites. If a sender does not exist at the recipient site as a remote user, a temporary remote user is added to the site with the sender's text name and spoken name.

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

Names Across the Network is now supported by VPIM Networking. Previously, only Enterprise Networking supported it.

Notes:

- You must coordinate with the network administrator of each remote site with which you want to enable NAN. NAN only works with remote sites that use Enterprise or VPIM Networking, and must be enabled on both the local messaging server and the remote servers.
- If you are using VPIM Networking, the NAN feature works even when the option is disabled for Enterprise Networking. NAN cannot be disabled for VPIM Networking.

For instructions on enabling Names Across the Network, refer to the CallPilot Manager online Help.

Network Message Service in multiple time zones

You can specify the time zone setting for each NMS satellite switch location that is associated with the local server. When the time zone for a satellite switch location is different from the time zone on the local server, time information is presented to the location's mailbox owners in the location's time zone.

Prior to CallPilot 2.0, time information for mailbox owners who were located in a different time zone from the CallPilot server were indicated in the CallPilot server's time zone.

Notes:

- Time information is presented in the form of message envelope information and CallPilot voice prompts.
- The prime switch location inherits its time zone setting from the local server. You cannot change it.

Network administration

The administration interface for CallPilot 2.0 and online Help for messaging network administration have been enhanced. Administration is now web-based, and requires the CallPilot Manager web server software. This guide provides a brief description of how to use CallPilot Manager to administer the messaging network. For more details, refer to the CallPilot Manager online Help.

Who should read this guide

Introduction

This guide was written for administrators who are responsible for configuring and maintaining the CallPilot messaging network.

Assumptions

This guide assumes that

- the CallPilot server has been correctly installed and is operational
- the switch has been installed and provisioned to support your CallPilot system
- the CallPilot networking services have already been configured, and your CallPilot system is communicating with other servers in the messaging network

IF	THEN
the CallPilot server has not been installed	install it before proceeding. For installation instructions, refer to Part 2 of the *Installation and Configuration* binder for your server model.
the CallPilot server has been installed but is not operational	refer to the following documents for information on troubleshooting your system: ■ Part 1 of the *Installation and Configuration* binder for your server model ■ *CallPilot Administrator's Guide* (NTP 555-7101-301)

IF	THEN
the networking services have not been configured	refer to the following CallPilot 1.0 networking guides: ■ *Networking Planning Guide* (NTP 555-7101-100) ■ *Implementation and Administration Guide* for each of the networking services you want to use For more details, see “Networking guides” on page 22.

Skills you need

Introduction

You need certain skills and knowledge to use this guide effectively.

Nortel Networks product knowledge

Knowledge of, or experience with, the following Nortel Networks products is beneficial:

- previous releases of CallPilot
- Meridian Mail

PC experience or knowledge

Knowledge of, or experience with, the following PC products is beneficial:

- Microsoft Windows NT
- Microsoft Windows 95
- Microsoft Windows 2000

Other experience or knowledge

Other types of experience or knowledge that may be of use include the following:

- switch configuration and operation (especially trunk group access restrictions [TGARs] and network classes of service [NCOS])
- network management
- client-server systems
- flowcharting
- troubleshooting

Related information products

Introduction

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

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

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

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

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

Planning and migration guides

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

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

Installation and configuration guides

The following guides describe how to install the following:

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

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

Administration guides

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

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

Document titles	NTP number
Application Builder Guide	555-7101-325
Desktop Messaging and My CallPilot Administration Guide	555-7101-503

Networking guides

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

Document titles	CallPilot release	NTP number
Networking Enhancements Guide	2.0	555-7101-507
Networking Planning Guide	1.0	555-7101-100
NMS Implementation and Administration Guide	1.0	555-7101-302
AMIS Networking Implementation and Administration Guide	1.0	555-7101-303
Enterprise Networking Implementation and Administration Guide	1.0	555-7101-304
Integrated AMIS Networking Implementation and Administration Guide	1.0	555-7101-305
VPIM Implementation and Administration Guide	1.0	555-7101-306

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

End user guides

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

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

Troubleshooting

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

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

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

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

Using online sources

CallPilot administration online Help

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

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

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

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

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

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

CallPilot end user online Help

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

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

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

Contacting technical support

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

Chapter 2

Planning the CallPilot network implementation

In this chapter

Overview

Introduction

This chapter provides an overview of the process and requirements for implementing CallPilot networking solutions. For more details, refer to the CallPilot 1.0 networking guides listed in “Networking guides” on page 22.

Networking solutions offered by CallPilot

The CallPilot networking solutions allow you to create a multimedia messaging network of up to 500 sites so that mailbox owners at one site can exchange messages with mailbox owners at other sites. Voice, fax, and text messages can be sent and received through the telephone or desktop PC.

Messages are transmitted from the local site to a remote site using one of the following protocols:

- AMIS Networking
- Enterprise Networking
- VPIM Networking

CallPilot can also exchange messages with users at sites that are not defined in your messaging network. Sites that are not defined in your messaging network are referred to as *open sites*. You can exchange messages with open sites using one of the following protocols:

- AMIS Networking (also referred to as Open AMIS Networking)
- VPIM Networking (also referred to as Open VPIM Networking)

In addition to these networking protocols, you can use Network Message Service (NMS). NMS allows two or more switches that are connected by ISDN to share the same messaging system. The users at each switch location have complete CallPilot functionality, and are all maintained on one CallPilot server. The collection of switch locations, connections, and the messaging server is known as an NMS network.

For more information about each of the networking solutions, refer to the guides listed in “Networking guides” on page 22, as well as the CallPilot Manager online Help.

AMIS Networking

AMIS Networking uses the Audio Messaging Interchange Specification-Analog (AMIS-A) protocol, an industry standard for the transmission of voice messages between messaging systems. You can use AMIS Networking to exchange voice messages with any remote sites that support the AMIS protocol. These remote sites can be within a private switch network (integrated sites), or within the public switch network (open AMIS sites).

Note: Remote sites that are configured to use the AMIS protocol in your network database are referred to as Integrated AMIS Networking sites.

Enterprise Networking

Enterprise Networking is a networking solution that transmits voice messages between mailbox owners at different sites in a private messaging network. Enterprise Networking uses a proprietary analog protocol that is based on extensions to the AMIS protocol.

If the Names Across the Network feature is enabled, Enterprise Networking also

- allows the local mailbox owner to hear a remote user’s spoken name while composing and sending messages
- supports the display of text names on the phoneset
- supports name dialing for remote addresses

VPIM Networking

VPIM Networking allows mailbox owners to exchange voice, fax, and text messages with other mailbox owners over a TCP/IP data network. You can use VPIM Networking to exchange messages with any remote site that supports the VPIM protocol. These remote sites can be part of your private network (integrated sites), or they can be in a public network (open VPIM sites). VPIM Networking uses Simple Message Transfer Protocol (SMTP) and Multipurpose Internet Mail Extensions (MIME) in compliance with the Voice Profile for Internet Mail (VPIM) standard.

About implementation

Implementation of CallPilot networking requires planning and coordination between the network administrators of the various sites. The time you spend planning the network saves you time during implementation. It also reduces the time it takes to troubleshoot network problems after implementation.

To properly plan for implementation, you must understand the process and what you are expected to do. You must also look at the implementation on paper. Analyze it to determine if there are any conflicts or missing information.

The complexity of the implementation depends on many factors, including the number of sites in the network and the type of dialing plan used.

The information in this chapter provides a general overview of the implementation process. More detailed information is located in the CallPilot 1.0 *Implementation and Administration Guide* for each networking solution. Read the relevant guides before beginning to implement any networking solution.

ATTENTION

You should understand all the information that you are expected to provide during implementation. You must coordinate this information with the network administrators of all other sites.

Note: For more information about the networking guides, see "Networking guides" on page 22.

Implementation scenarios

There are several possible scenarios for implementing your CallPilot system:

- Your site is part of a new messaging network of CallPilot systems.

  If you are designing a completely new messaging network in which each site uses CallPilot, you can design a simple and elegant messaging network.

  Preliminary planning must be done before you can install any networking solution. This planning results in a messaging network that is perfectly designed for CallPilot networking.

- Your site is being added to an existing, compatible messaging network.
- Your site is part of an existing messaging network that is being converted to CallPilot.

  If your site is part of an existing network that is being converted to CallPilot, the implementation process is somewhat different. For example, a dialing plan already exists. CallPilot networking is easiest to implement and maintain when the messaging network uses a uniform dialing plan. However, you will probably be unable to change the entire dialing plan to suit your preferences. Therefore, you may have to implement the networking solution or solutions using a dialing plan that is more complicated to implement and maintain. For more information about implementing a uniform dialing plan, refer to your switch documentation.

  If your site is being converted to CallPilot from Meridian Mail, you can migrate most of the existing information from Meridian Mail into the CallPilot network database. The Meridian Mail to CallPilot Migration Utility automates the movement of data. For more information, refer to the *Meridian Mail to CallPilot Migration Utility Guide* (NTP 555-7101-801).

- Your site is part of an existing messaging network and is being converted to CallPilot, while other sites are not being converted.

The process that you follow is determined somewhat by your particular situation. To simplify the process, follow the guidelines described in this guide, as well as in the CallPilot 1.0 networking *Implementation and Administration Guides* (see “Networking guides” on page 22).

Network administrators

A network administrator is responsible for the messaging network at one or more sites. You can designate

- one network administrator for all sites
- one network administrator for each site
- several network administrators, with each administrator being responsible for a small number of sites in the network

Your first step in planning is to determine who is responsible for implementing and administering a particular site.

ATTENTION

Nortel Networks recommends that one network administrator be responsible for coordinating the implementation and administration of the entire messaging network. Communication among site administrators is required to maintain the messaging network. A coordinator can simplify this process.

Installation and implementation concepts

Introduction

In CallPilot, a distinction is made between a networking solution that is installed and one that is implemented. The CallPilot 1.0 networking *Implementation and Administration Guides* (see "Networking guides" on page 22) describe in detail, the implementation process for each of the networking solutions.

This guide provides

- a general description of the implementation process and introduces some of the key concepts necessary to understand the process
- implementation checklists and configuration worksheets to help you plan and implement networking on your CallPilot server

Differences between installation and implementation

The difference between networking installation and implementation is important.

Installation

When you purchase the networking keycode, all networking solutions except NMS are installed and enabled on your CallPilot server.

Implementation

To be available on your server, the networking solution must be implemented. Implementation means that the networking solution is properly configured and the network database is set up.

Network implementation prerequisites

Implementation of a networking solution is an incremental activity. Before you begin to implement a networking solution, you must ensure that the following tasks are already completed:

- The CallPilot server is set up and configured for local use.

  If it is not, refer to the following documents for instructions:

  - *CallPilot Installation and Configuration* binder for your server
  - *CallPilot Administrator's Guide* (NTP 555-7101-301)
- The switch is set up and configured for local use.

  Note: Switch security features should be configured with networking in mind.
- The appropriate number of switch trunks are available.
- The appropriate number of CallPilot channels are available.

  For more details, refer to the CallPilot 1.0 *Networking Planning Guide* (NTP 555-7101-100).

Recommended order of implementation

Information that you provide when implementing one networking solution is also required when you implement the next networking solution.

For example, suppose you have Integrated AMIS Networking and Enterprise Networking installed on your system. Several configuration boxes that you must complete during the implementation of Integrated AMIS Networking are enabled because Enterprise Networking is also installed. In some instances, you must enter temporary information (which is called a placeholder), into those boxes before you can save the information in the network database.

The implementation process is easier if you follow this recommended order:

1. Network Message Service (NMS)
   For more information, refer to the CallPilot 1.0 *NMS Implementation and Administration Guide* (NTP 555-7101-302).
2. desktop or web messaging
   For more information, refer to the *Desktop Messaging and My CallPilot Installation Guide* (NTP 555-7101-505). For information about IMAP implementation, refer to the *Desktop Messaging and My CallPilot Administration Guide* (NTP 555-7101-503).
3. AMIS Networking, Integrated AMIS Networking, Enterprise Networking or VPIM Networking
   For more information, refer to the guides listed in "Networking guides" on page 22.

Network Message Service implementation

Nortel Networks recommends that you implement and test all NMS sites in the messaging network before you implement any other networking solution.

Nortel Networks also recommends that you verify the accuracy of information for your site before you release it to remote network administrators.

AMIS Networking

If your site uses the AMIS protocol to exchange messages with open sites only, implement AMIS Networking. Follow the procedures in the CallPilot 1.0 *AMIS Networking Implementation and Administration Guide*.

Integrated AMIS Networking

If your local site uses the AMIS protocol to exchange messages with only integrated sites, or with both integrated and open sites, implement Integrated AMIS Networking. Follow the procedures in the CallPilot 1.0 *Integrated AMIS Networking Implementation and Administration Guide*.

Implementation checklists

To help you track your progress while implementing one or more networking solutions, you can use the implementation checklists that are provided in Appendix A, "Implementation and planning tools":

- "AMIS Networking Implementation Checklist" on page 168
- "Integrated AMIS Networking Implementation Checklist" on page 171
- "Enterprise Networking Implementation Checklist" on page 174
- "VPIM Networking Implementation Checklist" on page 177
- "Open VPIM Implementation Checklist" on page 180

Designing the messaging network

Introduction

When you receive your CallPilot server, the basic design of your messaging network is already complete. The planning engineers who determined how CallPilot could be used in your messaging network also decided

- how many sites the messaging network will contain
- which networking protocols will be used

Basic design tasks for network administrators

You must complete the basic design of the messaging network. This includes the following tasks:

- Assign unique, useful names to every site in the messaging network.
- Identify the Network Message Service (NMS) sites in the messaging network.
- Determine the dialing plan that is used among sites.
- Determine the networking solution that will be used between a pair of sites.

Network database

Each site in the messaging network has its own network database that contains all information entered during the implementation and configuration of networking at that site. You must understand the network database structure because it is integral to understanding how to implement a networking solution.

The network database contains three main types of information:

- information about each of the networking solutions installed at the site
- information about the local site

- information about every remote site in the messaging network with which the local site communicates

The local site and each remote site that is configured in the network database consist of

- a messaging server—the computer on which CallPilot (or for remote sites, some other messaging system) resides
- a prime switch location—the switch that is directly attached to the messaging server

When the site uses NMS, the site configuration consists of

- a messaging server
- a prime switch location
- one or more satellite switch locations

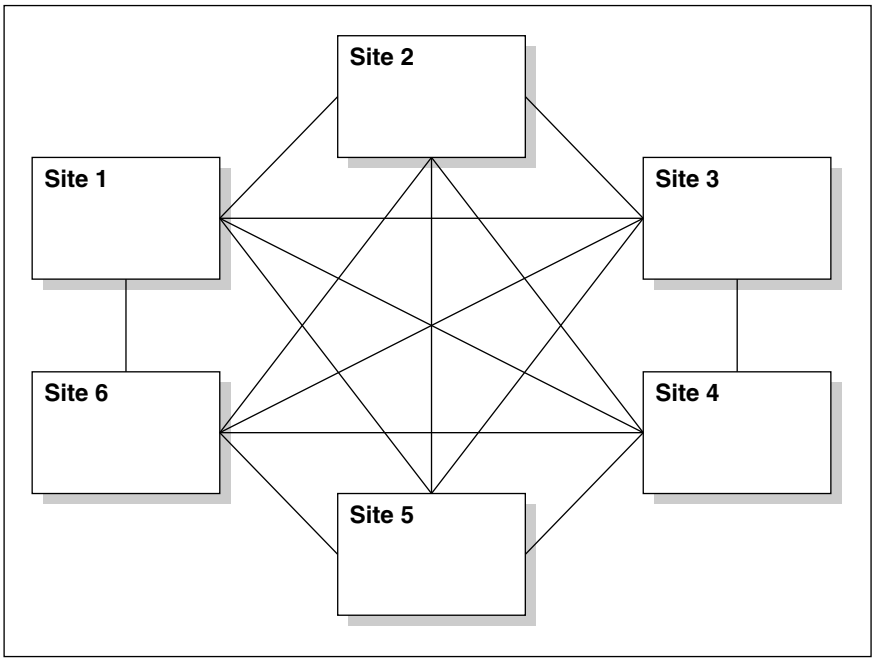
If a remote site is configured in the network database, it is considered to be an *integrated site*. If a remote site is not configured in the network database, it is considered to be an *open site*. For more details, see “Networking requirements and considerations” on page 45.

The information you enter into your network database for each remote site must be provided by the remote site’s network administrator. Most of the information that you enter for a remote site is the same information that is entered for the remote site in its network database. Network databases must be identical across the messaging network. Otherwise, networking will not work correctly.

When to add remote sites to the network database

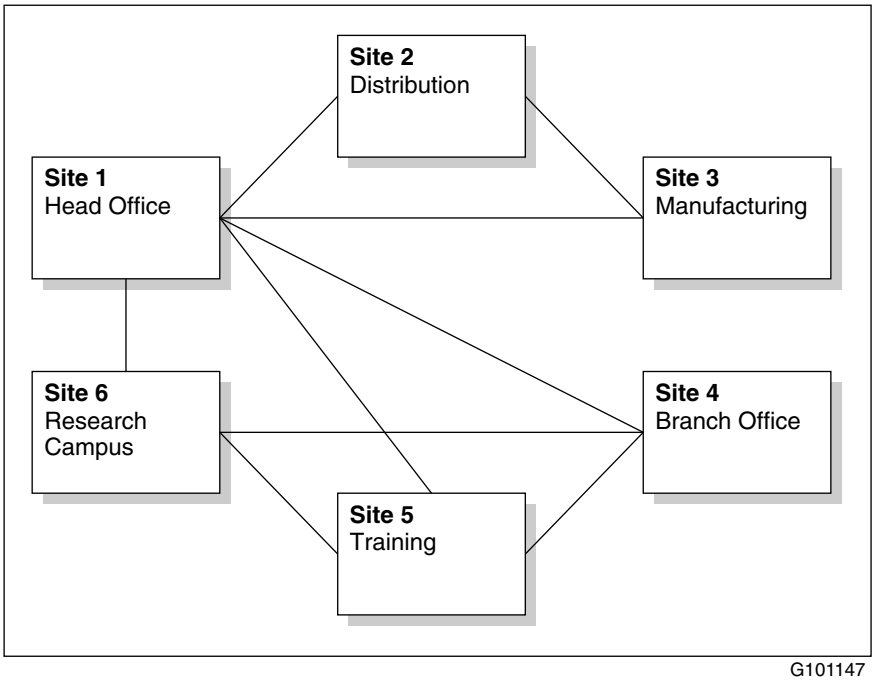
The local network database contains information about the remote sites with which the local site exchanges messages. These sites appear in the messaging network tree in CallPilot Manager.

If the messaging network is a true mesh network, your network database contains information about each site in the network. Each site can exchange messages with all sites in the network. See the following diagram:



For larger messaging networks, a mesh network may be impractical or unnecessary. In fact, in most messaging networks, a site connects only to those remote sites with which it commonly exchanges messages. In this case, the database does not contain the sites with which the local site does not exchange messages.

The following diagram illustrates a non-mesh network. In this example, only Head Office (site 1) connects to all sites. The other sites connect only to those sites with which messages are exchanged. The Manufacturing site, for example, connects only with the Distribution and Head Office sites.



The mesh or non-mesh network concepts are important because some values must be unique both in the network database and throughout the messaging network. When you configure CallPilot, CallPilot Manager can identify information that is not unique in the local network database. You must manually ensure that information is unique across the messaging network.

For more information about how CallPilot Manager validates information that you enter, see the following sections:

- “Validation” on page 74
- “Ensuring information is unique” on page 76

Open and integrated sites

The difference between open and integrated sites is one of the fundamental concepts in a messaging network.

A messaging network is made up of integrated sites. A site is considered integrated when it is included in the network databases of the other sites in the messaging network.

However, a site can exchange messages with sites that are not part of the messaging network. These sites are known as open sites. A typical open site can be a major customer or supplier to your company.

Protocols used to communicate with open sites

The ability to exchange messages with open sites is achieved by using industry-standard protocols, such as AMIS or VPIM. As long as the messaging system at an open site complies with either protocol, sites in the messaging network can communicate with the open site.

Implicit open sites

In addition to open and integrated sites, VPIM Networking uses the concept of implicit open sites.

You can use VPIM Networking in an integrated messaging network. Shortcuts for the VPIM Networking addresses of the remote sites with which you want to communicate are listed in your network database. These shortcuts enable users to address their messages using the telephone, because the shortcuts map to the address of the remote site. For more information about VPIM network shortcuts, refer to the CallPilot 1.0 *VPIM Implementation and Administration Guide* (NTP 555-7101-306), or the online Help in CallPilot Manager.

Coordinating network information

Introduction

If a network administrator makes changes to the configuration of one site, often these changes must be communicated to the network administrators of all other sites. The network databases of all other sites must reflect these changes.

Ensuring information is consistent across the network

One of the most important implications of the CallPilot network database system is the interdependence of the databases. Although each site has its own network database, the information in one must be consistent with the information contained in another. If you change one network database, you must ensure that all other network databases are also changed.

Therefore, network administrators must coordinate their efforts before implementing a networking solution or making changes. If changes are made to one network database but not to the other network databases, the messages exchanged with the site that changed its network database result in non-delivery notifications.

Information that must be coordinated

As part of the coordination effort, you must gather information for the whole network and analyze it to ensure that there are no conflicts or oversights. You must also coordinate the following information with the other network administrators before any site in the messaging network can be implemented:

- local messaging server name
- site ID
- protocol used between a pair of sites

- dialing plan used for connecting to each site
- connection information:
  - ESN location codes
  - CDP steering codes
  - connection DNs (Enterprise Networking) or system access numbers (AMIS Networking)
  - SMTP/VPIM network shortcuts (VPIM Networking)

Configuration worksheets

You can use the configuration worksheets, which are provided in Appendix A, "Implementation and planning tools," to record the information that you gather. You can then transfer this information to a messaging network diagram to help you visualize the network. Check the information carefully to ensure that each element is unique.

After all information is configured in CallPilot, you can

- retain the completed configuration worksheets as a hard copy backup record of your network
- send the completed worksheets to other messaging network administrators to help them configure the network databases at their sites

The following table identifies the configuration worksheets:

Information type	Worksheet name
CDP steering codes	"CallPilot Networking—CDP Steering Codes" on page 184
ESN location codes	"CallPilot Networking—ESN Location Codes" on page 186
your local site	"CallPilot Networking—Local Server Maintenance" on page 188

Information type	Worksheet name
each remote site	“CallPilot Networking—Remote Server Maintenance” on page 190
each switch location	“CallPilot Networking—Switch Location Maintenance” on page 192
your local server’s message delivery configuration settings	“CallPilot Networking—Message Delivery Configuration” on page 195
open VPIM shortcuts	“CallPilot Networking—Open VPIM Shortcuts” on page 199

Networking requirements and considerations

Introduction

When implementing a particular networking solution, consider the items discussed in this section. For more information, refer to the CallPilot 1.0 *Networking Planning Guide* (NTP 555-7101-100).

Interaction of networking with other CallPilot features

Each CallPilot networking solution supports different features. You must also be aware of how a particular networking solution interacts with other CallPilot features.

Dialing plans

When you begin to implement a networking solution, the dialing plan used by your local site is already configured on the switch. The decision about which dialing plan to use for each site in your network is already determined when you begin to implement a networking solution. Therefore, during implementation, you are simply reflecting the existing plan in your network database.

Even though the dialing plan is already set up, you must understand how to gather the dialing plan information from the switch. You must also understand the implications of the dialing plan for your messaging network.

Channel requirements

To process a call, every analog networking solution requires access to a channel. A channel provides a connection between the switch and the Digital Signal Processor (DSP) cards on the CallPilot server.

CallPilot supports three channel types, each corresponding to different media:

- voice
- fax
- speech recognition

Although a networking solution can work with all three types of channels, voice ports are usually used.

Note: VPIM Networking is transmitted over the TCP/IP network. Therefore, VPIM Networking does not require or use voice channels.

Network security

To maintain the integrity and security of your CallPilot system, each site in your messaging network should follow the recommended security precautions discussed in the CallPilot 1.0 *Networking Planning Guide* (NTP 555-7101-100).

Consider the following security measures:

- phoneset user, desktop user, and server access restrictions to prevent toll fraud

  Note: See also Chapter 4, “SMTP security,” in this guide.
- switch features, such as the following:
  - Trunk Group Access Restrictions (TGARs)
  - Class of Service (CLS)
  - Network Class of Service (NCOS)
- firewalls and packet filters (if you are using VPIM Networking)
- encryption (if you are using VPIM Networking)

  See Chapter 5, “Encryption,” in this guide.

Engineering considerations

You must consider the following engineering issues for each networking solution:

- the impact of VPIM Networking on the local area network (LAN)
- message handling capabilities of the networking solution (throughput)
- message queuing capacities
- message transmission times

Other considerations

Other considerations that you must be aware of are

- how many sites the messaging network can contain

  CallPilot supports a maximum of 500 integrated sites.
- how many delivery sessions can be active at one time

  The maximum number of simultaneous delivery sessions to a single remote site depends on the networking solution.
- the length to which mailbox numbers are limited

  For AMIS Networking, mailboxes cannot exceed 16 digits.
- how messages are handled

  All networking solutions deliver all messages in their entirety or not at all. Messages are never delivered in part. A non-delivery notification (NDN) indicates that no part of the message was received.

Chapter 3

Configuring the network with CallPilot Manager

In this chapter

Overview

Introduction

CallPilot Manager is a web-enabled administration tool that is used to configure and maintain your CallPilot server from any PC that has IP connectivity to your CallPilot server.

You can run CallPilot Manager using one of the following web browsers:

- Internet Explorer (version 5.0 or later)
- Netscape Communicator (version 6.2 or later)

CallPilot Manager provides two pages for implementing and maintaining the CallPilot networking solutions:

- Message Delivery Configuration
- Message Network Configuration

Message Delivery Configuration

The Message Delivery Configuration page is where message transmissions for each networking protocol are enabled, and settings such as the batch thresholds, delivery schedules, SMTP security, and encryption are defined.

Message Network Configuration

The Message Network Configuration page is where the local site, switch locations, and remote sites are defined.

Section A: Network administration concepts

In this section

Network views

Introduction

Your view of the messaging network depends on which site you are maintaining. From your perspective, only one site is local. All other sites are remote.

For example, suppose your network consists of five sites. From your perspective, your site is local while all others are remote. However, the administrator at a remote site sees its site as local and all others as remote.

Network views are relative

In most cases, the site where you are physically located is the local site. However, if the necessary permissions are set up on the system, you can administer a remote site. Even though the site is physically remote, from your perspective, it is the local site.

The following table provides some examples:

IF you are	THEN in the network database
located at Site 1	Site 1 is the local site; all other sites are remote sites.
located at Site 2	Site 2 is the local site; all other sites are remote sites.
dialing in to Site 2 and performing network administration from another site	Site 2 is the local site; all other sites are remote sites.

IF you are	THEN in the network database
dialing in to Site 1 and performing network administration from another site	Site 1 is the local site; all other sites are remote sites.

Performing local or remote administration

Introduction

You can implement and administer a CallPilot networking site either locally or remotely.

Local administration

In most networks, each site has an on-site messaging network administrator who is responsible for the system.

An on-site administrator has two advantages:

- The on-site administrator has a better understanding of the site's unique messaging requirements.
- The on-site administrator has a good understanding of the system.

However, there are some disadvantages to having an administrator at each site:

- Costs for maintaining the network are higher.
- There is an increased possibility that a change made at one site is not communicated quickly enough to all other site administrators.
- There is an increased likelihood of scattered network records, making it difficult to troubleshoot the system.

Remote administration

CallPilot's remote administration capability allows you to implement and administer sites remotely. If you are implementing and administering sites remotely, follow the procedures in this section for each site.

It is important to note, however, that whenever you are administering a site remotely, you are acting as the local administrator for that site.

Example: Remote site administration

Sandra Kapinski is the messaging network administrator of the New York site. The administrator of the Boston site is taking a temporary leave of absence. Sandra assumes responsibility for the Boston site from New York.

When Sandra administers the New York site, New York is the local server. When she administers the Boston site, Boston is the local server. Therefore, even though Sandra is physically in New York, when she administers the Boston site, she is acting as Boston's local administrator.

Site security

CallPilot protects site configuration from unauthorized users. To implement and administer sites remotely, you must have the proper authorization and password for each site.

Logging on to a local or remote server

You must use a web browser to log on to and administer the CallPilot 2.0 server. The process for logging on to a remote CallPilot 2.0 server is the same as for logging on to the local server. The logon process is completed in two stages:

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

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

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

   For example, if the CallPilot Manager web server's host name is Sunbird, the CallPilot Manager URL is http://sunbird/cpmgr/.

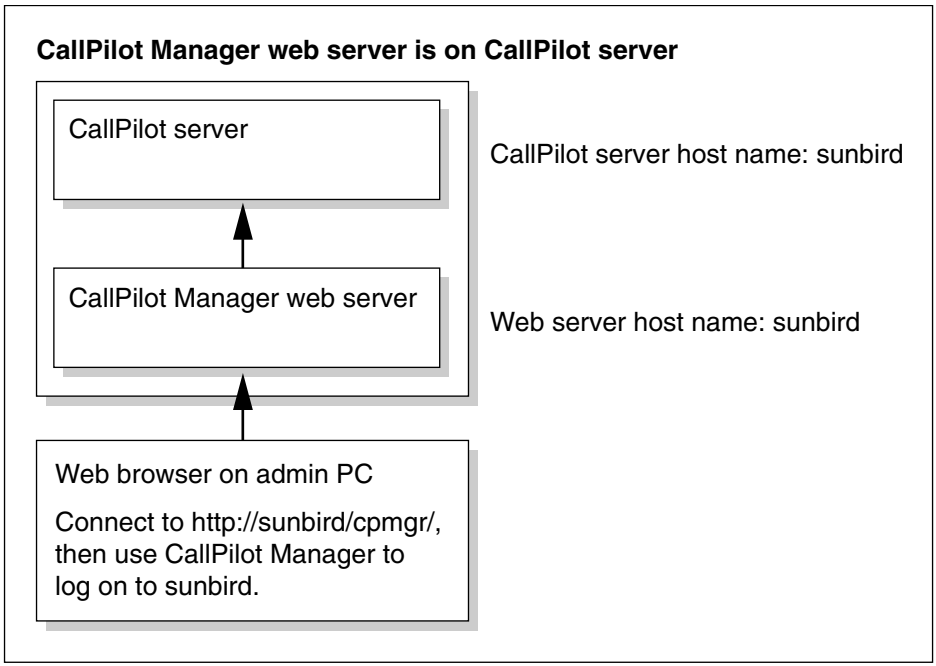
2. Log on to the CallPilot server with an administrator's mailbox number and password.

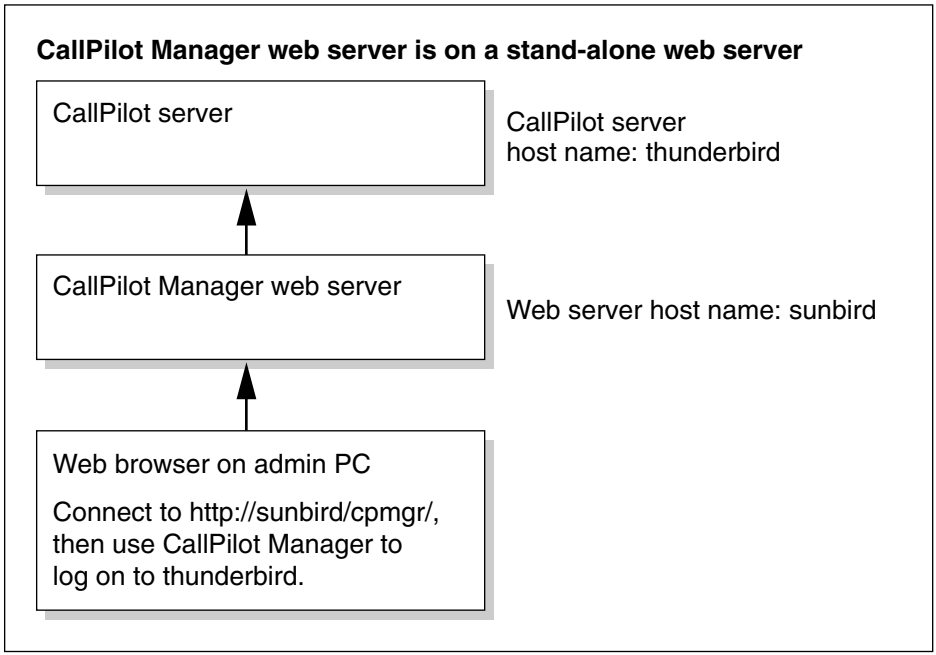
Note: You can use CallPilot Manager to log on to and administer any CallPilot 2.0 server in your network. You cannot use CallPilot Manager to administer CallPilot servers that are running CallPilot 1.07 or earlier.

Relationship of the CallPilot Manager web server to the CallPilot server

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

See the following diagrams.





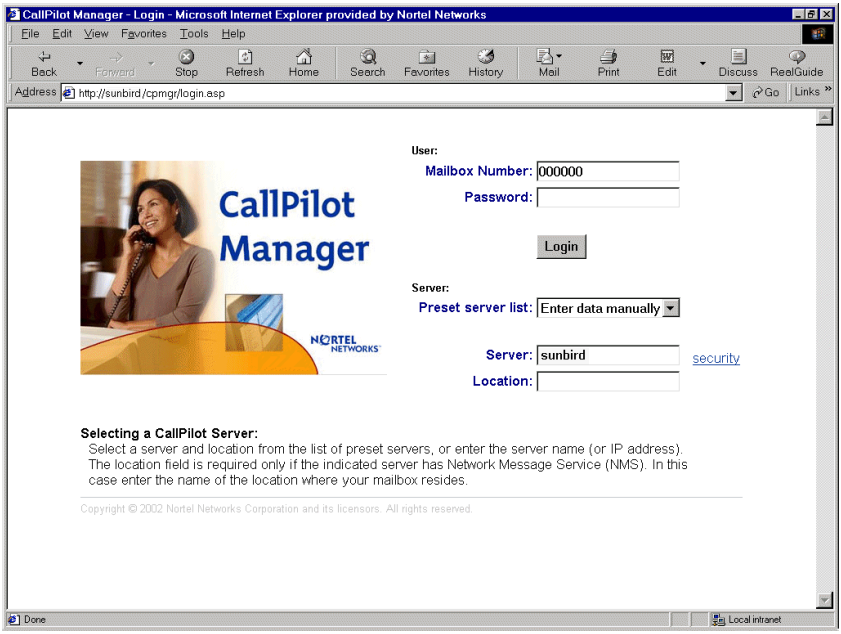
To log on to a local or remote server

1 Launch your web browser.

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

Example: http://sunbird/cpmgr/

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



3 Type the administrator mailbox number and password.

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

4 Do one of the following:

- Choose a server or location from the list of preconfigured servers or locations in the Preset server list box.
- Type the CallPilot server's host name or IP address in the Server box.
- If the CallPilot server you are connecting to has Network Message Service (NMS) installed, type the CallPilot server's host name or IP address in the Server box, then type the name of the switch location on which the administration mailbox resides in the Location box.

Note: Internet Explorer retains information that you have used before for each box except the Password. To reuse the information, do the following:

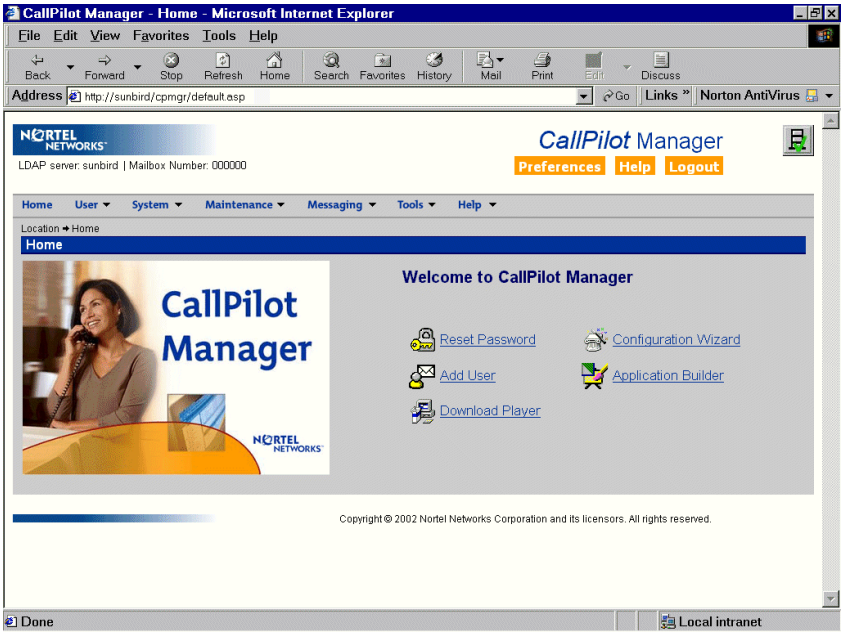
a. Clear the contents in the box.

b. Click once inside the box.

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

5 Click Login.

Result: The main CallPilot Manager page appears.



6 Work on the site as if you are working locally.

Multi-administrator environments

Introduction

Multiple administration is a standard database management feature that enables many administrators to work on a database at the same time.

There is no limit to the number of administrators who can work on the network database at the same time.

Advantages

Multiple administration offers several advantages, including

- shared knowledge of network database maintenance
- faster implementation

Refresh feature

More than one messaging network administrator can work on the configuration of satellite switch locations for a single site. Although this can cause confusion, you can avoid problems by taking advantage of the web browser's Refresh feature.

The Message Network Configuration tree does not automatically refresh the views for all messaging network administrators. For this reason, if you are working in a multiple administration environment, click the web browser's Refresh or Reload button frequently. This ensures that you see the most current tree.

Section B: CallPilot Manager networking configuration pages

In this section

Message Delivery Configuration description

Introduction

The Message Delivery Configuration page contains message delivery options information for each of the networking solutions. It is accessible in CallPilot Manager as follows:

- for all networking solutions if you purchased the networking feature
- for Enterprise Networking only, if you did not purchase the networking feature

Networking solutions

You must complete the Message Delivery Configuration page to implement the following networking solutions:

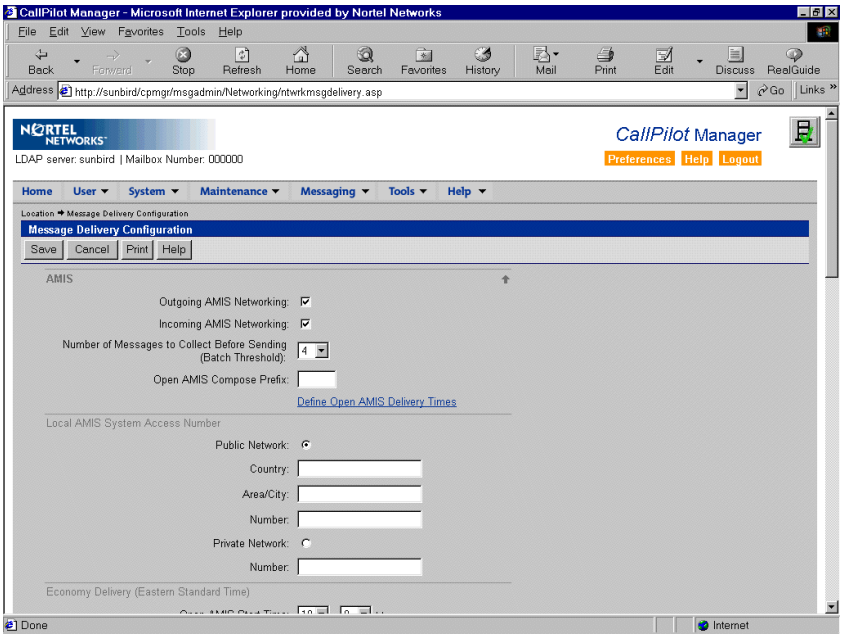
- AMIS Networking (open AMIS)
- Integrated AMIS Networking
- Enterprise Networking
- VPIM Networking (open VPIM)
- Integrated VPIM Networking

You do not use the Message Delivery Configuration page to implement NMS.

To open the Message Delivery Configuration page

In CallPilot Manager, click Messaging → Message Delivery Configuration.

Result: The Message Delivery Configuration page appears:



To navigate to subsequent pages

Some Message Delivery Configuration options are accessible on separate pages. To access the subsequent pages, click the underlined text on the main Message Delivery Configuration page, or the action button in the area you are configuring. When you click an underlined link or the action button, a new page appears.

To cancel changes on a CallPilot Manager page

Each page has a Cancel button. You must understand how Cancel works to ensure that you do not inadvertently lose configuration information that you have entered.

When you enter configuration information on a page, the information is only saved to the network database when you click Save.

This means that when you click Cancel, the following occurs:

- All of the changes that you enter on the page are deleted.
- You are returned to the previous page.

Click Cancel only if you want to undo all of your changes on the page.

Note: To delete specific information from a field, use the standard Windows methods, such as the Backspace or Delete keys.

To save configuration changes

You do not have to complete the configuration of your entire messaging network at one time. You must save any changes that you do make in a session. If you do not save your changes, the network database is not updated when you go to another CallPilot Manager page.

To save your changes, click Save on the page on which you are working.

To print the Message Delivery Configuration parameters

1 Click Print.

Result: A new browser window opens with the information in a format suitable for printing.

2 Click File → Print.

Result: The Print dialog box opens.

3 Specify the printing options as required, and then click OK.

Message Network Configuration description

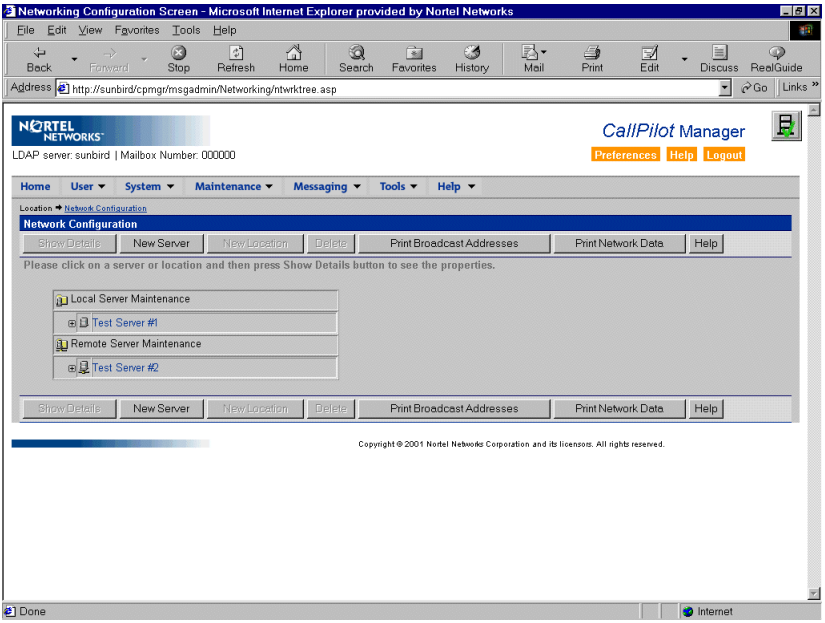
Introduction

The Message Network Configuration page contains a graphical representation of your messaging network. It uses a tree to show the local site and all remote sites in the messaging network. Use the tree to add, remove, and modify the configuration of messaging servers and switch locations in your messaging network.

To open the Message Network Configuration page

In CallPilot Manager, click Messaging → Message Network Configuration.

Result: The Message Network Configuration page appears, showing the network tree.



How sites and switch locations are represented

A site consists of a messaging server and a prime switch location. If the site is using NMS, the site also includes one or more satellite switch locations. In the tree view, a site is represented by the messaging server icon. To see the switch locations associated with a site, click the plus sign (+) next to the messaging server.

Note: To reduce the amount of time required to display the network tree, you can expand the tree for only one site at a time. This means that if the switch locations for a particular site are visible when you click another messaging server, the page refreshes to show only the switch locations for the messaging server that you chose.

Local messaging server and prime switch location

The local messaging server and local prime switch location are automatically added to the Message Network Configuration tree when CallPilot is installed on your system. They cannot be deleted.

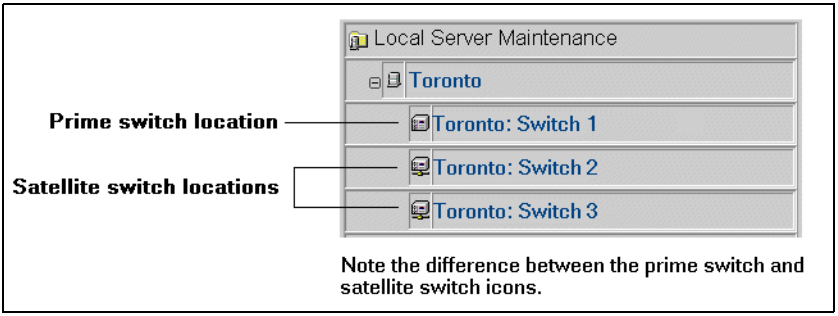
Remote messaging servers and prime switch locations

Each messaging server is associated with a prime switch location. For this reason, when you add a remote messaging server to your messaging network, a prime switch location is automatically created for that remote messaging server. By default, the prime switch location is given the same name as the messaging server. The prime switch location for a remote messaging server cannot be deleted.

Satellite switch locations

The messaging network tree shows which sites in the network are NMS sites. NMS sites have one or more satellite switch locations in addition to the prime switch location.

You can distinguish a prime switch location from a satellite switch location by its icon as follows:



Network tree and maximum number of sites

The Message Network Configuration tree can contain up to 500 sites. An NMS site can have up to 59 satellite switch locations.

Therefore, if CallPilot is used to its full capacity, your Message Network Configuration tree can contain 30 000 items. It is very important to be organized when implementing large messaging networks.

If the size of the network tree exceeds the size of the browser window, a scroll bar appears on the right side of the browser window.

Network tree organization

When you are implementing and maintaining large networks, it can be difficult to keep track of sites, messaging servers, and switch locations. For this reason, CallPilot automates some of the organization for you.

Local site

The local site is always shown at the top of the network tree, under the Local Server Maintenance branch.

If the local site is an NMS site, the prime switch location is always listed directly below the messaging server. The satellite switch locations are listed in alphabetical order below the prime switch location.

Remote sites

Remote sites are shown below the Remote Server Maintenance branch. Remote sites are listed in alphabetical order.

If the remote site is an NMS site, the first switch listed below the server is the prime switch. The satellite switches are listed in alphabetical order below the prime switch.

Working with the Message Network Configuration page

Introduction

Each messaging server and switch location in the Message Network Configuration tree has a page that contains the configuration settings for that messaging server or switch location.

To open a messaging server or switch location page

You can open the page for any messaging server or switch location in the messaging network from the Message Network Configuration tree.

1 In CallPilot Manager, click Messaging → Message Network Configuration.

2 Do one of the following tasks:

To	Click
add a new remote server	New Server. **Result:** A blank page for the new messaging server appears.
add a new switch location	the name of the messaging server in which you are interested, and then click New Location. **Result:** A blank page for the switch location appears.
modify the configuration for an existing server or switch location	the name of the messaging server or switch location in which you are interested, and then click Show Details. **Result:** The page for the messaging server or switch location appears.

3 Configure the settings on the page as required.

For instructions, refer to the CallPilot Manager online Help.

4 Click Save.

To navigate to subsequent pages

Some Message Network Configuration options are accessible on separate pages. To access these pages, click the underlined text on the main Message Network Configuration page, or the action button in the area you are configuring. When you click an underlined link or the action button, a new page appears.

To cancel changes on a CallPilot Manager page

Each page has a Cancel button. You must understand how Cancel works to ensure that you do not inadvertently lose configuration information that you have entered.

When you enter configuration information on a page, the information is only saved to the network database when you click Save.

This means that when you click Cancel, the following occurs:

- All of the changes that you enter on the page are deleted.
- You are returned to the previous page.

Click Cancel only if you want to undo all of your changes on the page.

Note: To delete specific information from a field, use the standard Windows methods, such as the Backspace or Delete keys.

To save configuration changes

You do not have to complete the configuration of your entire messaging network at one time. You must save changes that you do make in a session. If you do not save your changes, the network database is not updated when you go to another CallPilot Manager page.

To save your changes, click Save on the page on which you are working.

To delete a server or switch location

ATTENTION

You cannot delete the following:

- local messaging server and its prime switch location
- prime switch location for a remote messaging server

1 In the network tree, click the messaging server or switch location that you want to delete.

2 Click Delete.

Result: You are prompted to confirm the deletion.

3 Click OK.

To print the information for all sites

You can print the contents of your Message Network Configuration tree. This can be an important part of your messaging network history. Store dated printouts with your messaging network diagram and other records.

1 On the main Message Network Configuration page, click Print Network Data.

Result: A new browser window opens with the information in a format suitable for printing.

2 Click File → Print.

Result: The Print dialog box opens.

3 Specify the printing options as required, and then click OK.

To print the broadcast addresses used by a local switch location

1 On the main Message Network Configuration page, click Print Broadcast Addresses.

Result: The Print Broadcast Addresses page appears, listing the following:

- local broadcast address
- network broadcast address
- location broadcast address for each switch location that is associated with the local server

  Users at the local prime location must use these addresses when they want to send broadcast messages to a specific switch location.

2 In the Location list box, choose the location for which you want to view location broadcast addresses.

Note: The list box contains only the locations that are associated with the local server.

Result: The Print Broadcast Addresses page refreshes with the location broadcast addresses that users at that switch location must use when they want to send a broadcast message to another switch location.

3 To print the broadcast addresses, click Print.

Result: A new browser window opens, with the broadcast address list in a format suitable for printing.

4 Click File → Print.

Result: The Print dialog box opens.

5 Specify the printing options as required, and then click OK.

Validation

Introduction

Validation is the process of checking the information entered during configuration before saving it to the database. Validation identifies any problems with the information that you have entered before it is added to the network database. This minimizes configuration problems and helps to ensure that the information you have entered works.

Levels of validation

There are two levels of validation:

- field
- record

Field validation

Field validation ensures that you can enter only valid characters into a box on a page. For example, if a box accepts only numbers, you are not allowed to enter letters.

If you are unable to enter characters into a box and do not know why they are being rejected, click the Help button on the page. The online Help appears explaining what the page does, as well as identifying its default values and restrictions, if any.

Record validation

Record validation ensures that the information you have entered while completing a page is complete and consistent, and does not conflict with any other records in the network database. Record validation occurs when you click Save.

Examples

Many boxes must be unique within the site. If a site uses the Coordinated Dialing Plan (CDP), you can define up to 500 steering codes. Each steering code must be unique for the site. However, other sites can use the same steering codes.

Other boxes must be unique across the messaging network. For example, each messaging server must have a unique name and site ID.

For more information, see “Ensuring information is unique” on page 76.

Ensuring information is unique

Introduction

As you configure the messaging network, you must provide information that is unique. When determining if information is unique, you must consider two factors:

- the context in which an item is unique
- the comparison against which an item is unique

Context

There are different contexts in which an item must be unique:

- Some items must be unique for the local site.

  Example: CDP steering codes
- Other items must be unique in the local network database (which contains the local site and all remote sites with which the local site exchanges messages).

  Example: Site ID
- An item may have to be absolutely unique in the context of certain other items.

  Example: Network shortcuts and prefixes (For more details, see “Unique numbers” on page 77.)

Uniqueness and validation

It is important to keep the uniqueness requirements in mind when implementing a messaging network, because not all boxes are automatically validated for uniqueness.

Whenever a box must be unique against local information or information in the local network database, it is automatically validated. If a box is not unique as required, an error is generated and you must correct the information before it is accepted.

Note: Several boxes (such as the site ID and connection DNs) must be synchronized across the entire messaging network. The information in various network databases cannot be checked automatically. For these types of boxes, the network administrators of all sites must coordinate their efforts and determine if the information entered in each network database is correct. This must be done before implementation begins, ideally as part of the information-gathering phase of the implementation process.

Unique numbers

Most of the information that must be unique is numerical. In a messaging network, unique numbers have a particular definition.

A unique number is one that does not conflict with another number. Conflict occurs when there is an exact or a partial match when compared from left to right. A number is unique when it does not repeat any consecutive digits when read from left to right.

Example

- 6338 conflicts with 6338, 633, 63, and 6.
- If you use 6338 and require a unique number, you must use one that is unique from left to right; for example, 7338 is unique.

Time periods

Introduction

When you implement CallPilot networking solutions, several parameters are expressed as periods of time.

24-hour clock

CallPilot uses a 24-hour clock. Therefore, 3:00 p.m. is expressed as 15:00.

Guidelines

Use the following guidelines to specify time periods:

- The last minute of any hour is expressed as *x*:59 (where *x* represents the hour).

  For example, 8:00–8:00 is actually configured as 8:00–7:59.
- Overlapping time periods are affected accordingly.
  - There is no overlap between 8:00–10:00 (configured as 8:00–9:59) and 10:00–17:00 (configured as 10:00–16:59).
  - There is a 1-minute overlap between 8:00–10:00 (configured as 8:00–9:59) and 9:59–17:00 (configured as 9:59–16:59).

Chapter 4

SMTP security

In this chapter

Overview

Introduction

CallPilot uses Simple Mail Transport Protocol (SMTP) to send

- VPIM Networking messages between the local CallPilot server and remote CallPilot servers
- VPIM Networking messages between the local CallPilot server and remote messaging servers that are VPIM compliant
- messages from desktop messaging and My CallPilot users to the CallPilot server

In CallPilot, the component that implements SMTP is known as the Internet Mail Agent.

Simple Mail Transport Protocol authentication

CallPilot supports SMTP authentication, which is a hacker and toll fraud prevention method. CallPilot authenticates message transmission sessions from the following:

- desktop messaging and My CallPilot users
- voice messaging servers that have been defined as remote sites in the CallPilot network database

Two methods of authentication are supported:

- Challenge and Response authentication, using the CRAM-MD5 algorithm
- User ID and Password authentication

For more information about the authentication methods, see “SMTP authentication methods” on page 91.

This guide focuses on SMTP authentication and messaging activity between remote messaging servers and CallPilot. For more information about SMTP, desktop messaging, and My CallPilot activity, refer to the CallPilot Manager online Help.

Modes of authentication

You can configure SMTP authentication in one of the following modes on CallPilot:

- unauthenticated mode

  CallPilot does not request authentication from a sender. Therefore, message senders are never authenticated.

  Note: CallPilot, however, can limit the addressing capabilities of the sender by enforcing the unauthenticated access restrictions for users and servers, if they are configured.

- authenticated mode

  CallPilot always requests authentication. Successful authentication must occur before the message can be transmitted.

  You enable authentication by choosing one or both of the following authentication methods:

  - Challenge and Response
  - User ID and Password

- mixed authentication mode

  Authentication is optional. It is performed only if it is supported at both ends of the connection. If authentication is not being performed, CallPilot may limit the addressing capabilities of the sender by enforcing the unauthenticated access restrictions for users and servers, if they are configured.

  If authentication is being used, and it fails, the session is disconnected.

  You enable mixed authentication by choosing both the unauthenticated mode, and one or both of the following authentication methods:

  - Challenge and Response
  - User ID and Password

ATTENTION

When defining the authentication settings, remember that the settings also affect the addressing capabilities of desktop messaging and My CallPilot users who want to compose messages.

Monitoring suspicious SMTP activity

You can use one of the following methods to monitor suspicious SMTP and VPIM Networking activity:

- review SMTP-related events in the Windows NT event log (automatic monitoring)

  If you choose to use the Windows NT event log as your monitoring method, no action is required from you to initiate SMTP/VPIM monitoring.

- enable monitoring of activity from specific origins on the Security Administration page in CallPilot Manager (manual monitoring)

  You can enable activity monitoring based on the following:

  - authenticating user ID

    The user ID can be either a user's public switch telephone (PSTN) number (SMTP/VPIM shortcut and mailbox number) or a remote server's authenticating FQDN.

  - IP address of the remote messaging server, desktop messaging user, or My CallPilot user that is attempting to connect to the CallPilot server
  - FQDN of the remote messaging server, desktop messaging user, or My CallPilot user that is attempting to connect to the CallPilot server

Encryption

Optionally, you can use encryption to secure all message traffic. Encryption prevents

- password transmission in the clear
- eavesdroppers from gaining access to the contents of the message (thereby guaranteeing user privacy)

CallPilot networking, desktop messaging, and My CallPilot use encryption. Encryption is enabled and configured independently from SMTP authentication configuration.

For more information about encryption, see Chapter 5, “Encryption.”

Unauthenticated mode

Introduction

In unauthenticated mode, CallPilot does not request authentication from a sender. The Internet Mail Agent (SMTP) transports message without authentication

- from a remote voice messaging server to the CallPilot server
- from a desktop messaging or My CallPilot user to the CallPilot server

How to enable unauthenticated mode

The unauthenticated mode is enabled by default when you install or upgrade your CallPilot server.

When to use the unauthenticated mode

Use the unauthenticated mode if

- you are not experiencing problems with inappropriate access
- you do not want to use SMTP authentication in your network
- the desktop messaging or My CallPilot clients used in your organization do not support SMTP authentication
- your messaging network contains
  - messaging servers that do not support SMTP authentication
  - VPIM-compliant sites that are not defined in CallPilot's network database (open VPIM sites)

    Note: Open VPIM sites can use only the unauthenticated mode when connecting to CallPilot.

Preventing denial-of-service attacks and junk e-mail in unauthenticated mode

To prevent denial-of-service attacks and junk e-mail proliferation, Nortel Networks recommends that you restrict the following from remote messaging servers that are not authenticated:

- incoming messages that are addressed to shared distribution lists (SDLs)
- incoming location and network broadcast messages

  Note: You can block incoming network broadcasts from a specific network site or all sites in the network database. This capability is in addition to the SMTP authentication feature, and is discussed in "CallPilot server capabilities for broadcast messages" on page 138.
- the number of recipients on incoming messages

  This prevents hackers from copying the contents of a large address book into the recipient list. The limit applies to all recipients within the message, including recipients in nested messages.

  CallPilot enforces the limit separately on each of the TO, CC, and Blind CC lists. For example, if the limit is defined as 100, the sender can enter 100 addresses in each of these recipient lists.

  If any recipient list exceeds the recipient limit, CallPilot rejects the entire message.

If CallPilot rejects a message as a result of any of these restrictions, the sender receives a non-delivery notification (NDN).

Preventing toll fraud

ATTENTION

To prevent toll fraud by desktop messaging and My CallPilot users who are not authenticated, Nortel Networks recommends that you restrict user addressing capabilities and the number of recipients on outgoing messages. These restrictions are enforced by

- unauthenticated desktop user restrictions on the Unauthenticated Access Restrictions page in CallPilot Manager
- the desktop restriction/permission list (RPL)
- mailbox class

For more information about these items, refer to the CallPilot Manager online Help.

Authenticated mode

Introduction

Authentication verifies the authenticity of the sender, which can be a desktop messaging user, My CallPilot user, or a remote messaging server.

In authenticated mode, CallPilot always requests authentication from the sender. Successful authentication must occur before the message is transmitted and received by the CallPilot server.

SMTP authentication can also be performed on outgoing sessions to remote servers. The receiving system advertises the methods it supports, and CallPilot responds accordingly. If authentication fails, the CallPilot SMTP server attempts to send the message without authentication. If the receiving system rejects any SMTP commands, the connection is dropped, and a non-delivery notification is generated.

How to enable the authenticated mode

To enable authenticated mode, you choose one or both of the following authentication methods in CallPilot Manager:

- Challenge and Response
- User ID and Password

For more information about the authentication methods, see page 91.

When to use the authenticated mode

SMTP authentication provides maximum security in which spoofing is virtually impossible. You can only use the authenticated mode when all messaging servers in the network, desktop messaging clients, and My CallPilot clients support authentication.

SMTP authentication is supported in closed networks only. SMTP authentication cannot be performed between CallPilot and open VPIM sites (that is remote messaging servers that are *not* defined in the CallPilot network database). If the message transmission session cannot be authenticated, the messages themselves cannot be transmitted.

Note: You must use the mixed authentication mode if

- your voice messaging network contains messaging systems, desktop messaging clients, and My CallPilot clients that do not support SMTP authentication
- your users want to receive messages from open VPIM sites

For more details, see "Mixed authentication mode" on page 89.

Denial-of-service attacks, junk e-mail, and toll fraud

The authenticated mode prevents denial-of-service attacks, junk e-mail, and toll fraud. Therefore, it is not necessary to enforce the restrictions that are described in

- "Preventing denial-of-service attacks and junk e-mail in unauthenticated mode" on page 85
- "Preventing toll fraud" on page 86

Mixed authentication mode

Introduction

In mixed authentication mode, SMTP authentication is optional. CallPilot requests authentication, but does not require it for a successful connection.

Authentication is performed only if it is supported at both ends of the connection. If authentication is not supported, CallPilot accepts the message without authentication, but limits the addressing capabilities of the sender.

How to enable mixed authentication

To enable mixed authentication, you choose both of the following in CallPilot Manager:

- unauthenticated mode
- one or both of the following authentication methods:
  - Challenge and Response
  - User ID and Password

By default, unauthenticated mode and Challenge and Response are both enabled.

When to use mixed authentication

Use mixed authentication if your messaging network contains any of the following:

- VPIM-compliant sites that are not defined in CallPilot's network database
- messaging servers that support SMTP authentication
- messaging servers that do not support SMTP authentication

- desktop messaging or My CallPilot clients that support authentication
- desktop messaging or My CallPilot clients that *do not* support authentication

CallPilot accepts messages from both authenticated and unauthenticated senders, but restricts the capabilities of senders that are not authenticated.

How mixed authentication affects users

In mixed authentication mode, message receipts and hence, user addressing capabilities are affected as follows:

When the server or user is	incoming messages
unauthenticated	■ from remote servers can be blocked as described in "Preventing denial-of-service attacks and junk e-mail in unauthenticated mode" on page 85 ■ from desktop messaging or My CallPilot users can be restricted as described in "Preventing toll fraud" on page 86
authenticated	do not have to be blocked. The restrictions for users and remote servers *are not* enforced. **Note:** Users are still restricted to the capabilities allowed in their mailbox classes.

When you *should not* use mixed authentication

If you are concerned about security, Nortel Networks recommends that you use the authenticated mode only.

SMTP authentication methods

Introduction

CallPilot supports the following SMTP authentication methods:

- Challenge and Response
- User ID and Password

The method used to perform SMTP authentication on a remote server, desktop messaging client, or My CallPilot client depends on what is supported by both the sending and receiving systems. If both authentication methods are supported, the sending system chooses the authentication method.

Challenge and Response authentication is the preferred method on CallPilot because it provides authentication with inherent encryption and is, therefore, always secure.

ATTENTION

Nortel Networks recommends that if you want to use the User ID and Password authentication method, you also use Secure Socket Layer (SSL) to encrypt the connection. SSL encryption prevents password transmission in the clear and ensures content privacy while the message is in transit.

For more information about encryption, see Chapter 5, “Encryption.”

Note: Authentication of remote servers can occur only if the remote server is defined in the CallPilot network database. Open VPIM sites cannot be authenticated.

Challenge and Response authentication process

The Challenge and Response authentication method uses the CRAM-MD5 algorithm. The following steps describe the Challenge and Response authentication process for an incoming message session:

1. The sending system (remote server, desktop messaging user, or My CallPilot user) connects to the CallPilot Internet Mail Agent (SMTP server).
2. CallPilot advertises that it supports Challenge and Response authentication.
3. One of the following occurs:

IF the sending system	THEN
supports Challenge and Response authentication	the sending system requests authentication.
does not support Challenge and Response authentication	authentication fails and the message transmission is handled as described in “Authentication failures” on page 95.

4. CallPilot generates and passes a string containing a time stamp and other text.
5. The sending system generates and sends a response that contains the string, user ID, and password.
   - For a desktop messaging or My CallPilot user, the user ID is the user's PSTN number (SMTP/VPIM shortcut and mailbox number). The password is the mailbox password.
   - For a remote messaging server, the user ID is the remote server’s fully qualified domain name (FQDN). The password is the server’s SMTP/VPIM password.

6. CallPilot generates a string that contains the user ID and password.
   - For a desktop messaging or My CallPilot user, the mailbox and user password are obtained from the user database.
   - For a remote messaging server, the remote server's FQDN and SMTP/VPIM password are obtained from the network database.
7. CallPilot compares the two strings.

IF the strings	THEN
match	the sending system is authenticated and message transmission continues.
do not match	authentication fails and the message transmission is handled as described in "Authentication failures" on page 95.

User ID and Password authentication process

The following steps describe the User ID and Password authentication process for an incoming message session:

1. The sending system (remote server, desktop messaging user, or My CallPilot user) connects to the CallPilot Internet Mail Agent (SMTP server) through either the SMTP port or the SSL port.

   Notes:

   - By default, 465 is defined as the SSL port that listens for encrypted sessions. Port 25 listens for unencrypted sessions.
   - The CallPilot SMTP server does not require SSL on incoming transmissions, but does support it. On outgoing sessions, SSL must be enabled if User ID and Password authentication is being used.
2. CallPilot advertises that it supports user ID and password authentication.

3. One of the following occurs:

IF the sending system	THEN
supports User ID and Password authentication	the sending system requests authentication.
does not support User ID and Password authentication	authentication fails and the message transmission is handled as described in “Authentication failures” on page 95.

4. CallPilot requests the user ID.
5. The sending system responds with the user ID:
   - For a desktop messaging or My CallPilot user, the user ID is the user’s PSTN number (SMTP/VPIM shortcut and mailbox number).
   - For a remote messaging server, the user ID is the remote server’s FQDN.
6. CallPilot requests the password.
7. The sending system responds with the password.
8. CallPilot verifies the user ID and password:
   - For a desktop messaging or My CallPilot user, the mailbox and user password are obtained from the user database.
   - For a remote messaging server, the remote server’s FQDN and SMTP/VPIM password are obtained from the network database.

IF the user ID and password	THEN
match	the sending system is authenticated and message transmission continues.
do not match	message transmission is handled as described in “Authentication failures” on page 95.

Authentication failures

Introduction

This section describes

- situations in which SMTP authentications can fail
- what happens when SMTP authentication failures occur

You can specify the maximum number of authentication failures that can occur from remote messaging servers, desktop messaging users, or My CallPilot users.

You can also specify what CallPilot should do when the number of failed authentication attempts exceeds the maximum limit that you specify.

When authentication can fail

SMTP authentication can fail in the following situations:

- Passwords are not configured correctly in CallPilot Manager for the local CallPilot server and the remote messaging server.
- The user's user ID, password, or both are not configured correctly in the desktop messaging or My CallPilot client.
- The requested authentication method is not supported at both ends of the connection.

  This can occur when
  - a desktop messaging or My CallPilot user is using a desktop client or web browser that does not support SMTP authentication at all
  - the desktop messaging or My CallPilot user is using a client or web browser that does not support the SMTP authentication method requested by CallPilot
  - the remote messaging server does not support SMTP authentication

- the remote messaging server does not support the SMTP authentication method requested by CallPilot

What happens when authentication fails

CallPilot cannot receive messages when authenticated mode only is used and authentication fails. If mixed authentication is being used on CallPilot, a message transmission can still occur *without* authentication.

Incoming messages from desktop messaging or My CallPilot users

For incoming messages from desktop messaging or My CallPilot users, the message must leave the user's outbox and be received by the CallPilot server before CallPilot can deliver the message to the destination.

IF CallPilot is configured to use	THEN
authenticated mode only, and authentication fails for an incoming message from a desktop messaging or My CallPilot user	the message remains in the user's outbox in the desktop messaging client or web browser. An NDN is not sent to the user because the user can immediately determine that the message was not sent.
mixed authentication, and authentication fails for an incoming session from a desktop messaging or My CallPilot user	the message remains in the user's outbox in the desktop messaging client or web browser. An NDN is not sent to the user because the user can immediately determine that the message was not sent.
mixed authentication, and authentication is not attempted for an incoming message from a desktop messaging or My CallPilot user	CallPilot accepts the message *without* authentication. The unauthenticated desktop user restrictions are enforced. See "Preventing toll fraud" on page 86.

Incoming messages from remote servers

IF CallPilot is configured to use	THEN
authenticated mode only, and authentication fails for an incoming VPIM Networking message transmission	CallPilot drops the connection. The sender may receive an NDN if the remote server supports NDNs.
mixed authentication, and authentication fails for an incoming VPIM Networking session	CallPilot drops the connection. The sender may receive an NDN if the remote server supports NDNs.
mixed authentication, and authentication is not attempted for an incoming VPIM Networking message transmission	CallPilot accepts the message *without* authentication. The unauthenticated server restrictions are enforced. See "Preventing denial-of-service attacks and junk e-mail in unauthenticated mode" on page 85.

Outgoing messages to remote messaging servers

When an initiating SMTP password is defined on your CallPilot server, SMTP authentication is performed on outgoing sessions to remote servers. If authentication is attempted and fails, CallPilot still attempts to send the message. If the advertised authentication method is not supported, CallPilot attempts to send the message without authentication.

If the outgoing message was initiated by a desktop messaging or My CallPilot user, the unauthenticated desktop user restrictions are enforced. See "Preventing toll fraud" on page 86.

If the remote server rejects any SMTP commands, and the message cannot be sent after several attempts, CallPilot sends an NDN to the sender and logs an event.

What happens when there are too many failed authentication attempts

You can specify the maximum number of failed authentication attempts that can occur from remote messaging servers, desktop messaging users, or My CallPilot users, and what action to perform when the limit is exceeded. You can choose to

- report the event in the event log and generate an alarm
- disable the remote messaging server in your network database and report the event

  When the remote server is disabled, the following results occur:
  - CallPilot rejects all incoming VPIM messages from that server (both authenticated and unauthenticated). This prevents hackers from trying all the possible password combinations and eventually obtaining the correct password.
  - If unsuccessful authentication attempts continue, CallPilot reports an event for each time the maximum number of failed attempts is exceeded.
- disable the user's mailbox and report the event

  When the user's mailbox is disabled, CallPilot rejects the following from the user:
  - all mailbox logon attempts (including logon attempts from a phoneset)
  - all incoming VPIM messages from a desktop messaging or My CallPilot client that is configured as belonging to the user

  This prevents hackers from trying all the possible password combinations and eventually obtaining the correct password.

  CallPilot also reports an event for each time the maximum number of failed attempts is exceeded.

To allow CallPilot to receive incoming messages again, you must reenable the remote server in your network database or the user's mailbox in user administration.

Enabling CallPilot SMTP authentication

Introduction

To enable SMTP authentication between CallPilot and remote messaging servers, you must configure specific options on both the local server and on each remote server in the CallPilot network database that is using VPIM Networking. The procedures in this section identify the tasks that you must complete.

To enable SMTP authentication between CallPilot, desktop messaging users, and My CallPilot users, you must also configure the desktop messaging and My CallPilot clients. For instructions on configuring the desktop messaging and My CallPilot clients, refer to the *Desktop Messaging and My CallPilot Administration Guide* (NTP 555-7101-503).

To configure the SMTP authentication options on the local server

1. In CallPilot Manager, click Messaging → Message Delivery Configuration.
2. In the SMTP/VPIM section, click Security Modes for SMTP Sessions.

   Result: The Security Modes for SMTP Sessions page appears.
3. If the User ID and Password authentication method is used, specify the options in the Encryption Options section.

   Note: For more information, see Chapter 5, “Encryption.”

4 In the Authentication Options section, specify the required options:

Option	Description
Unauthenticated	Choose this option if you do not want to request SMTP authentication from desktop messaging users, My CallPilot users, and remote servers in your messaging network. When checked, CallPilot accepts messages from unauthenticated desktop messaging users, My CallPilot users, and remote servers. **Note:** If unauthenticated mode is used, Nortel Networks recommends that you also enable unauthenticated access restrictions for servers and desktop users.
Challenge/Response Authentication	Choose this option if you want CallPilot to request SMTP authentication using the CRAM-MD5 challenge and response algorithm.
User ID/Password Authentication	Choose this option if you want CallPilot to request SMTP authentication using the User ID and Password algorithm. **Note:** Nortel Networks recommends that you also enable encryption to prevent password transmission in the clear.
SMTP/VPIM Password for Initiating Authenticated Connections to Remote Servers	If authentication is used, type the password that CallPilot should send when initiating outgoing message transmissions to remote servers. The password should ■ contain a minimum of 6 characters ■ be mixed uppercase and lowercase ■ contain both letters and digits or special characters Maximum length: 30 alphanumeric characters

Option	Description
SMTP/VPIM Password for Initiating Authenticated Connections to Remote Servers (continued)	**Note:** A blank password means that CallPilot does not attempt to perform SMTP authentication when connecting to remote servers.

5 If authentication (or mixed authentication) is used, specify options for failed authentication in the Authentication Failure Attempts section:

Option	Description
Maximum failed authentication attempts from a remote server	Type a number to identify how many times a remote server can fail SMTP authentication before an event is logged.
Action to perform when the maximum has been reached	Choose one of the following options: ■ Log only: To report an event in the event log only. ■ Log and Disable Server: To report an event in the event log and disable incoming message receipts from the server that failed SMTP authentication. When the remote server is disabled, CallPilot rejects all incoming VPIM messages from that server (both authenticated and unauthenticated). This prevents hackers from trying all the possible password combinations, and eventually obtaining the correct password. If unsuccessful authentication attempts continue, CallPilot reports an event for each time the maximum number of failed attempts is exceeded.

Option	Description
Maximum failed authentication attempts from a user	Type a number to identify how many times a desktop messaging or My CallPilot client can fail SMTP authentication before an event is logged.
Action to perform when the maximum has been reached	Choose one of the following options: ■ Log only: To report an event in the event log only. ■ Log and Disable User: To report an event in the event log and disable the mailbox belonging to the desktop messaging or My CallPilot user that failed SMTP authentication. When the user's mailbox is disabled, CallPilot rejects the following from the user: ■ all attempts to log on to the mailbox (including logon attempts from a phoneset) ■ all incoming VPIM messages from a desktop messaging or My CallPilot client that is configured as belonging to the user This prevents hackers from trying all the possible password combinations, and eventually obtaining the correct password. CallPilot also reports an event for each time the maximum number of failed attempts is exceeded.

6 Click Save.

Result: You are returned to the Message Delivery Configuration page.

7 If unauthenticated mode is being used, you should enable restrictions for incoming messages from unauthenticated users and servers. For instructions, see "Configuring unauthenticated access restrictions" on page 104.

To configure the SMTP authentication options on each remote server

1 In CallPilot Manager, click Messaging → Message Network Configuration.

2 In the Remote Server network tree, click the remote server that you want to modify.

Result: The page for the remote server appears.

3 Ensure that VPIM is selected in the Network Protocol box.

4 In the VPIM Security section, configure the following:

Option	Description
SSL port number	If encryption is used, type the port number designated as the Secure Socket Layer port on the remote messaging server. Default: 465 When the SSL port is specified, and if the Connect to server with SSL for Outgoing SMTP Sessions option is enabled in Message Delivery Configuration, CallPilot attempts to establish an encrypted connection with this port when connecting to this remote server.
Server password	Type the SMTP authentication password that the remote server must send when the local CallPilot server requests SMTP authentication. Maximum length: 30 alphanumeric characters
Receive messages from this server	Choose Enabled from the list box to allow the local server to receive messages from this remote server.

5 Click Save.

Configuring unauthenticated access restrictions

Introduction

If unauthenticated mode is used, Nortel Networks recommends that you also enable unauthenticated access restrictions for servers and desktop users.

To configure unauthenticated access restrictions for users

1 In CallPilot Manager, click Messaging → Message Delivery Configuration.

2 In the SMTP/VPIM section, click Unauthenticated Access Restrictions.

Result: The Unauthenticated Access Restrictions page appears.

In the Unauthenticated Desktop User Restrictions section, select the capabilities available to unauthenticated users:

Option	Description
Delivery to Telephone or Fax	Choose this option if you want to allow desktop messaging and My CallPilot users to send Delivery to Telephone (DTT) or Delivery to Fax (DTF) messages. When checked, users are still constrained by the desktop restriction/permission list and their own mailbox class restrictions. This option is cleared by default.

Option	Description
Enable Open AMIS	Choose this option if you want to allow desktop messaging and My CallPilot users to address messages to open AMIS sites. When checked, users are still constrained by the desktop restriction/permission list and their own mailbox class restrictions. This option is cleared by default. **Note:** If AMIS Networking is not enabled on CallPilot, this option is not available.
Enable Integrated Networking	Choose this option if you want to allow desktop messaging and My CallPilot users to address messages to users at integrated sites. When checked, users are still constrained by the desktop restriction/permission list and their own mailbox class restrictions. This option is cleared by default.
Enable SDL Addressing	Choose this option if you want to allow desktop messaging and My CallPilot users to address messages to shared distribution lists. When checked, users are still constrained by their own mailbox class restrictions. This option is cleared by default.
Enable Broadcast Addressing	Choose this option if you want to allow desktop messaging and My CallPilot users to address messages to location broadcast or network broadcast addresses. When checked, users are still constrained by their own mailbox class restrictions. This option is cleared by default.

Option	Description
Restrict Recipients	Choose this option if you want to limit the number of recipients that a message from a desktop messaging or My CallPilot user can contain. This prevents hackers from copying the contents of a large address book into the recipient list. The limit applies to all recipients within the message, including recipients in nested messages. This option is cleared by default. When cleared, CallPilot allows messages that contain any number of recipients.
Maximum Recipients	Type a number to identify how many recipients the message can contain in each of the TO, CC, and Blind CC recipient lists. CallPilot enforces the limit separately on each for each address list. For example, if the limit is defined as 100, the user can enter 100 addresses in each of the TO, CC, and Blind CC recipient lists. If any recipient list exceeds this limit, CallPilot rejects the entire message and sends a non-delivery notification (NDN) to the user. Range: 0 (no restrictions on the number of recipients) to 999 (maximum of 999 recipients)

3 Continue with “To configure unauthenticated access restrictions for servers” on page 107.

To configure unauthenticated access restrictions for servers

1 In the SMTP/VPIM section, click Unauthenticated Access Restrictions.

Result: The Unauthenticated Access Restrictions page appears.

2 In the Unauthenticated Server Restrictions section, select the capabilities available to unauthenticated servers:

Option	Description
Enable SDL Addressing	Choose this option if you want CallPilot to accept messages from remote servers that are addressed to shared distribution lists. This option is cleared by default. When cleared, CallPilot rejects messages addressed to shared distribution lists and sends non-delivery notifications (NDNs) to the senders.
Enable Broadcast Addressing	Choose this option if you want CallPilot to accept messages from remote servers that are addressed to location broadcast or network broadcast addresses. This option is cleared by default. When cleared, CallPilot rejects messages addressed to broadcast addresses and sends non-delivery notifications (NDNs) to the senders. You can also block incoming network broadcasts from a specific network site or all sites in the network database. This capability is in addition to the SMTP authentication feature. For more information, see Chapter 6, “Network and location-specific broadcast messages.”

Option	Description
Restrict Recipients	Choose this option if you want to limit the number of recipients that a message from a remote server can contain. This prevents hackers from copying the contents of a large address book into the recipient list. The limit applies to all recipients within the message, including recipients in nested messages. This option is cleared by default. When cleared, CallPilot allows messages that contain any number of recipients.
Maximum Recipients	Type a number to identify how many recipients the message can contain in each of the TO, CC, and Blind CC recipient lists. CallPilot enforces the limit separately on each for each address list. For example, if the limit is defined as 100, the sender can enter 100 addresses in each of the TO, CC, and Blind CC recipient lists. If any recipient list exceeds this limit, CallPilot rejects the entire message and sends a non-delivery notification (NDN) to the sender. Range: 0 (no restrictions on the number of recipients) to 999 (maximum of 999 recipients)

3 Click Save.

See also

You should perform the following additional tasks, as required:

- Configure the desktop restriction/permission lists (RPLs).
- Assign RPLs to a mailbox class.
- Assign message delivery options to mailbox class members.

For instructions, refer to the CallPilot Manager online Help.

Monitoring suspicious SMTP activity

Introduction

You can use one of the following methods to monitor suspicious SMTP and VPIM Networking activity:

- review SMTP-related events in the Windows NT event log (automatic monitoring)

  If you choose to use the Windows NT event log as your monitoring method, no action is required from you to initiate SMTP/VPIM monitoring.
- enable monitoring of activity from specific origins on the Security Administration page in CallPilot Manager (manual monitoring)

Automatic monitoring

Automatic monitoring alerts you to suspicious SMTP activity, blocks access to the system, and provides sufficient information for further investigation. No configuration is required for automatic SMTP/VPIM monitoring.

How it works

If CallPilot detects repeated unsuccessful authentication attempts (for example, an incorrect password is presented), the following events occur:

- for a local user: after the specified number of unsuccessful attempts, an event is logged in the Windows NT event log and, if configured, the user's mailbox is disabled.

  If the mailbox is disabled, the user cannot log on either from a phoneset or by using a desktop messaging or My CallPilot client. Messages are no longer accepted via SMTP from that user, regardless of whether the user is authenticated or not.

- for a remote server: after the specified number of unsuccessful attempts, an event is logged in the Windows NT event log and, if configured, message reception from the remote server is disabled.

  If the remote server is disabled, messages from the remote server are no longer accepted.

Note: If the sender presents itself as a local mailbox or a remote server that does not actually exist, the system treats it the same way 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 in the Windows NT event log. The event includes the following information:

- the User ID used in the authentication attempt

  The user ID can be either a user's public switch telephone (PSTN) number (SMTP/VPIM shortcut and mailbox number) or a remote server's authenticating FQDN.
- the hostname and IP address from which the last authentication failure occurred

You can use this information to investigate the source of the suspicious activity, or enable manual hacker monitoring.

Monitoring activities manually

You can manually monitor activity based on the following information:

- the authenticating user ID
- the IP address of the remote messaging server, desktop messaging client, or My CallPilot client that is attempting to connect to the CallPilot server
- the FQDN of the remote messaging server, desktop messaging client, or My CallPilot client that is attempting to connect to the CallPilot server

You can define up to 100 activities to monitor. When you enable monitoring, the system provides you with a detailed list of activities received from the user ID, IP address, 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. For more information, refer to the following in the *CallPilot Administrator's Guide* (NTP 555-7101-301):

- "Configuring messaging service defaults"
- "Throttling and customizing events"

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.

  Note: This retains the activity in the list so that you can enable it again, if required.

Using wildcards

Wildcards are not supported when creating activity specifications.

To enable manual monitoring of SMTP/VPIM activities

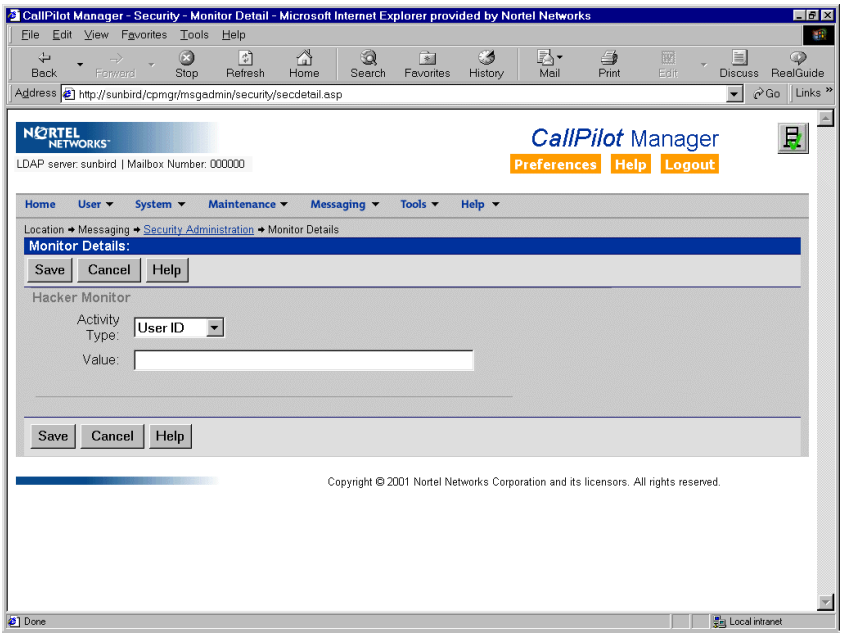
1 In CallPilot Manager, click Messaging → Security Administration.

2 In the SMTP/VPIM section, ensure the Enable Monitoring Activities check box is checked.

Result: This enables monitoring of all checked items in the Activities to Monitor list.

3 Click Add.

Result: The Activity Monitor page appears.



4 Choose one of the following items from the Activity Type list box:

- User ID
- IP Address
- FQDN

5 Type the value that should be monitored in the Value box.

Note: The value for User ID can be either the mailbox owner's SMTP/VPIM prefix and mailbox number, or a remote server's FQDN.

6 Click Add.

Result: The system returns you to the Security Administration page.

7 In the SMTP/VPIM section, check the item you just added, and then click Save.

Chapter 5

Encryption

In this chapter

CallPilot encryption description

Introduction

CallPilot supports Secure Socket Layer (SSL) encryption to encrypt message transmissions between CallPilot and

- desktop and web messaging clients
- another messaging server

Privacy guarantee

When you use SSL to encrypt message traffic between messaging servers, users are provided with privacy over the network.

Total privacy is obtained only when

- the message originates from a phoneset, or SSL is used between the desktop or web messaging client and the CallPilot server
- SSL is used end-to-end between messaging servers
- the SSL transaction is successful

When to use encryption

Encryption is optional. However, Nortel Networks strongly recommends that you establish a secure (encrypted) session if you use the User ID and Password authentication method. User ID and password transmission in the clear is strongly discouraged.

Encryption prevents

- password transmission in the clear
- eavesdroppers from gaining access to the contents of the message (thereby guaranteeing user privacy)

Considerations for implementing encryption

To determine whether you need to implement encryption in your CallPilot network, consider the following questions:

- Is encryption needed for secure desktop or web messaging logon?
- Is encryption required between messaging servers?
- Does your network infrastructure support secure message transmission from end to end?

  If messages cross a firewall or pass through an intermediate mail relay, encryption may not be provided end-to-end.
- Do you need to upgrade any systems?

TCP/IP traffic encryption for SSL requires significant CPU resources. The impact of using SSL depends on

- total network traffic (desktop and VPIM)
- percentage of traffic that is using SSL

Secure transmission of a message to a remote CallPilot system is pointless if the message is also addressed to another system that does not support SSL. To do so wastes CPU bandwidth.

How CallPilot encryption works

Introduction

The CallPilot SMTP server monitors port 25 for non-encrypted SMTP sessions. The CallPilot SMTP server also monitors (and connects to) port 465 for encrypted sessions. Encryption is provided by enabling Secure Socket Layer (SSL), which is also known as Transport Layer Security (TLS).

SSL sessions can be established only when SSL is supported at both ends of the connection.

SSL port monitoring

When SSL is enabled, the CallPilot server listens on port 465 for SSL handshake protocol commands. If the remote host sends a request for a connection to this port but does not provide the SSL handshake commands, the session cannot be established.

Similarly, if SSL is required, the CallPilot SMTP server attempts to connect to the SSL port on a remote messaging server. The default SSL port is 465.

SSL with User ID and Password authentication

The following table describes how SSL and the User ID and Password authentication method work together to guarantee user privacy over the network:

IF	THEN
SSL is enabled on the local server	message transmission sessions are encrypted. ■ For outgoing sessions, the CallPilot SMTP server attempts to connect to the SSL port on the remote messaging server. If the connection is successful, the session is encrypted to prevent password transmission in the clear. ■ For incoming sessions, the CallPilot SMTP server listens for non-encrypted connections on port 25 and encrypted connections on port 465 from remote SMTP hosts. If the connection is successful, the session is encrypted to prevent password transmission in the clear.
SSL is not enabled on the local server	message transmission sessions are not encrypted. ■ For outgoing sessions, the CallPilot SMTP server establishes the connection with the remote messaging server, but does not try to authenticate. The session continues without authentication to prevent password transmission in the clear. If the remote server requires authentication, then message transmission will not occur.

IF	THEN
SSL is not enabled on the local server (continued)	■ For incoming sessions, the CallPilot SMTP server listens for connections from remote SMTP hosts on port 25 only.
the SSL connection cannot be established on an incoming connection (encryption fails)	the CallPilot SMTP server drops the connection. Message transmission does not occur.
the SSL connection cannot be established on an outgoing connection (encryption fails)	the CallPilot SMTP server drops the connection. CallPilot sends a non-delivery notification (NDN) to the message originator.

CallPilot encryption and Meridian Mail Net Gateway

Meridian Mail Net Gateway encryption (using Entrust) is not supported by CallPilot. Therefore, message transmissions between CallPilot and a Meridian Mail Net Gateway system cannot be encrypted.

CallPilot encryption and VPIM-compliant systems

The SMTP connection is encrypted if

- SSL is enabled at both ends
- encryption certificates are accepted by each system

Intermediate mail relays and application proxy servers must participate in the establishment of secure sessions.

Encryption, authentication, mail relays, and firewalls

SSL encryption (and authentication) works best when messages are transferred point-to-point (for example, within a firewall).

When messages are not transmitted point-to-point, SSL sessions may still be initiated and authentication may still be performed if the firewalls are configured appropriately. It may also be possible to initiate SSL sessions between intermediary mail relays and proxies if those systems support SSL and are configured appropriately. However, end-to-end authentication may not be possible.

CallPilot encryption and certificates

SSL implementation requires a certificate on the CallPilot server. The CallPilot SMTP server uses the certificate that is provided for Internet Message Access Protocol (IMAP) and Lightweight Directory Access Protocol (LDAP). No specific manual interventions are required by you to create a certificate for SMTP.

Notes:

- Some third-party VPIM-compliant messaging systems may or may not accept the CallPilot certificate. Therefore, it may be necessary to use third-party certificates. The availability of compatible encryption algorithms can limit the use of SSL between some systems.
- You may need to use a certificate import feature to import certificates created from known certificate authorities, such as Verisign.

The CallPilot SMTP server accepts *all* certificates when establishing an SSL session. That is, CallPilot does not verify the digital signature. Therefore, establishing the secure session does not guarantee that CallPilot is actually sending the message to a specific destination.

For example, a tampered router in the network can redirect messages to a server that is spoofing a known site. CallPilot cannot verify that the certificate presented by the remote site is legitimate, and sends the encrypted message to the rogue server, which can decrypt the message with its master keys.

Implementing encryption on CallPilot

Introduction

This section describes how to configure the encryption options on the CallPilot server for both the local server and each remote server that is defined in the CallPilot network database.

For instructions on how to configure the encryption options in desktop or web messaging clients, refer to the *Desktop Messaging and My CallPilot Installation Guide* (NTP 555-7101-505).

ATTENTION

Ensure that SSL is available on all systems, including intermediate systems such as gateways, mail relays, and so on. For information about implementing encryption on network devices, refer to the device manufacturer's documentation.

How encryption is implemented

Encryption is enabled and configured independently from SMTP authentication configuration. (For information about SMTP authentication, see Chapter 4, "SMTP security.")

SSL configuration consists of the following tasks:

1. On the local server:
   - Enable SSL for incoming sessions from desktop or web messaging clients and remote messaging systems.
   - Enable SSL for outgoing message transmission sessions to remote messaging systems.
2. For each remote server defined in the CallPilot network database, specify the port that the CallPilot server connects to establish an SSL session.

To enable SSL encryption on the local server

1. In CallPilot Manager, click Messaging → Message Delivery Configuration.
2. In the SMTP/VPIM section, click Security Modes for SMTP Sessions.

   Result: The Security Modes for SMTP Sessions page appears.
3. In the Encryption Options for SMTP Sessions section, specify the required options:

Option	Description
Enable SSL for incoming SMTP Sessions	Choose this option if you want to establish secure connections with incoming connecting SMTP hosts. When enabled, the CallPilot SMTP server listens on port 465 for encrypted connection requests. The SMTP server also listens on port 25 for unencrypted connection requests.
Connect to server with SSL for Outgoing SMTP Sessions	Choose this option if you want to encrypt outgoing VPIM Networking message transmission sessions with remote messaging servers. When enabled, the CallPilot SMTP server attempts to initiate secure connections with the SSL port on remote SMTP hosts. **Note:** If the “Enable SSL for incoming SMTP Sessions” check box is cleared, this option is not available.

4. Click Save.

To enable SSL encryption for each remote server

1. In CallPilot Manager, click Messaging → Message Network Configuration
2. In the Remote Server network tree, choose the remote server that you want to modify.
3. In the Connections section, ensure that VPIM is selected in the Network Protocol list box.
4. In the VPIM Security section, type the number of the port that has been designated as the SSL port on the remote messaging server.

   By default, this is 465.

   When the SSL port is specified, and if the Connect to server with SSL for Outgoing SMTP Sessions option is enabled in Message Delivery Configuration, CallPilot attempts to establish an encrypted connection with this port when connecting to this remote server.
5. Ensure that the other VPIM security options are configured as required.
6. Click Save.

Chapter 6

Network and location-specific broadcast messages

In this chapter

Types of network broadcasts

Introduction

The CallPilot network broadcast feature enables a phoneset, or desktop or web messaging user to send a broadcast message to

- all users at a specific network location (location broadcast)
- all users in the network (network broadcast)

This feature is in addition to the existing broadcast feature, which allows local users to send a broadcast message to all local users on the CallPilot server (local broadcast).

Broadcast requirements

To send a broadcast message, the following criteria must be met:

- The message must be addressed to the appropriate broadcast address.

  If the local user wants to send a broadcast message to all NMS locations associated with a remote site, the user must address the message to each location. To simplify this task, the user can create a personal distribution list containing the location-specific broadcast address for each location.

  Note: Broadcast addresses cannot be added to shared distribution lists (SDLs).
- The user must have sufficient capabilities as determined by his or her mailbox class.
- Broadcast messages must be enabled between the local CallPilot server and remote voice messaging systems.
- Broadcast messages must be supported on both the local CallPilot server and remote voice messaging system. For more information, see “Broadcast messages in a mixed messaging network” on page 142.

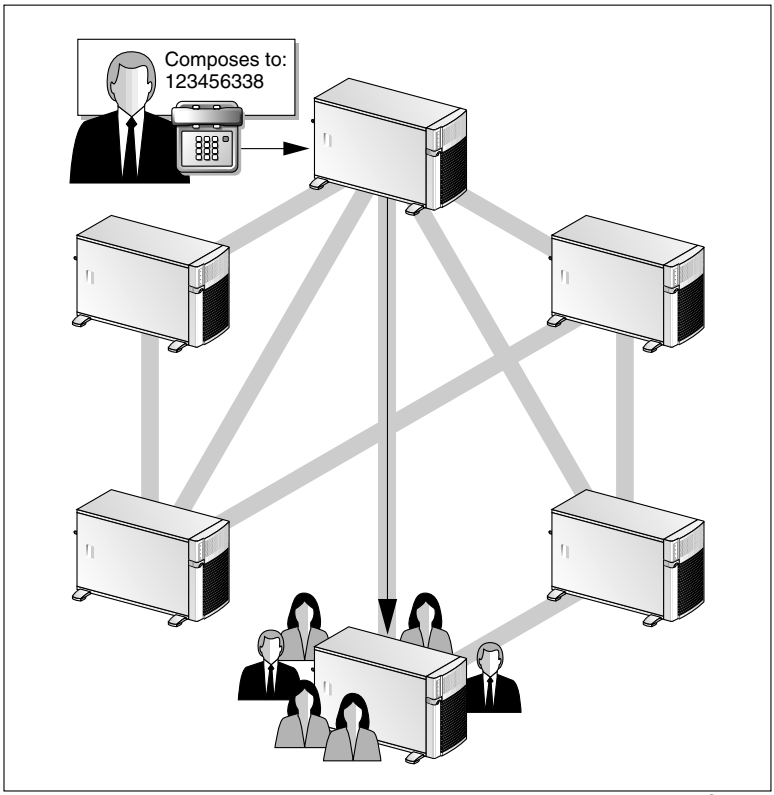
Location broadcast

When a user sends a location broadcast, the message is delivered only to the users at the specified location. In this context, the location can be a remote site, or it can be a Network Message Service location associated with either a local or remote site.

See the following diagrams.

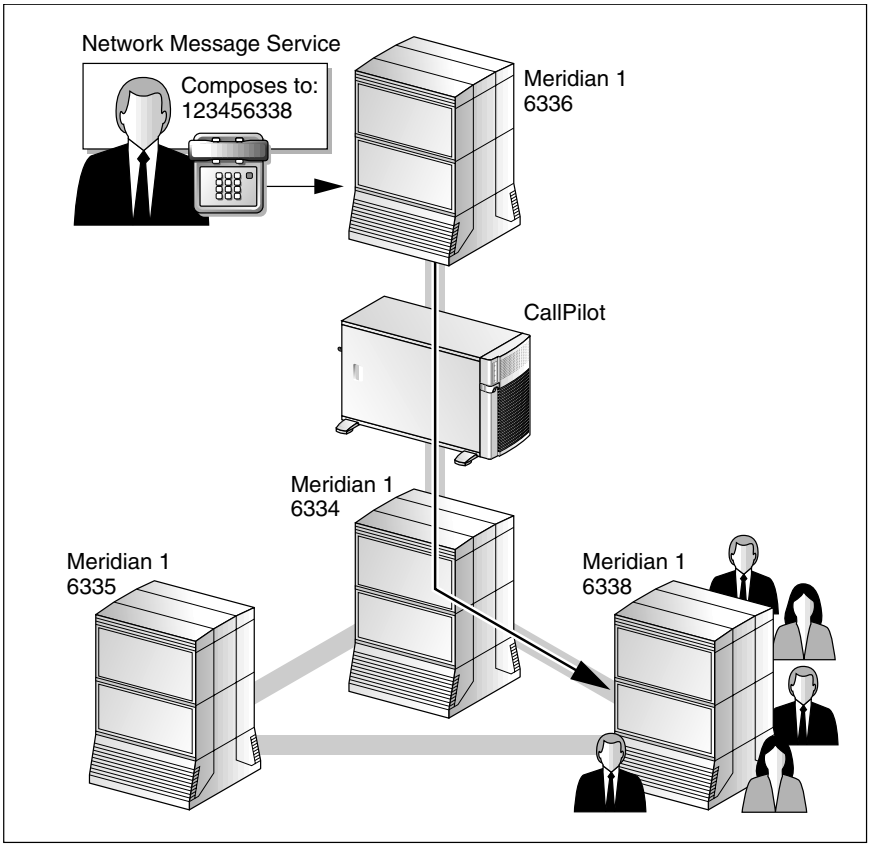
Broadcast sent to a specific remote site

In the following diagram, 12345 is the network broadcast prefix, and 6338 is the location prefix defined in the network database for the prime switch location at the remote site:



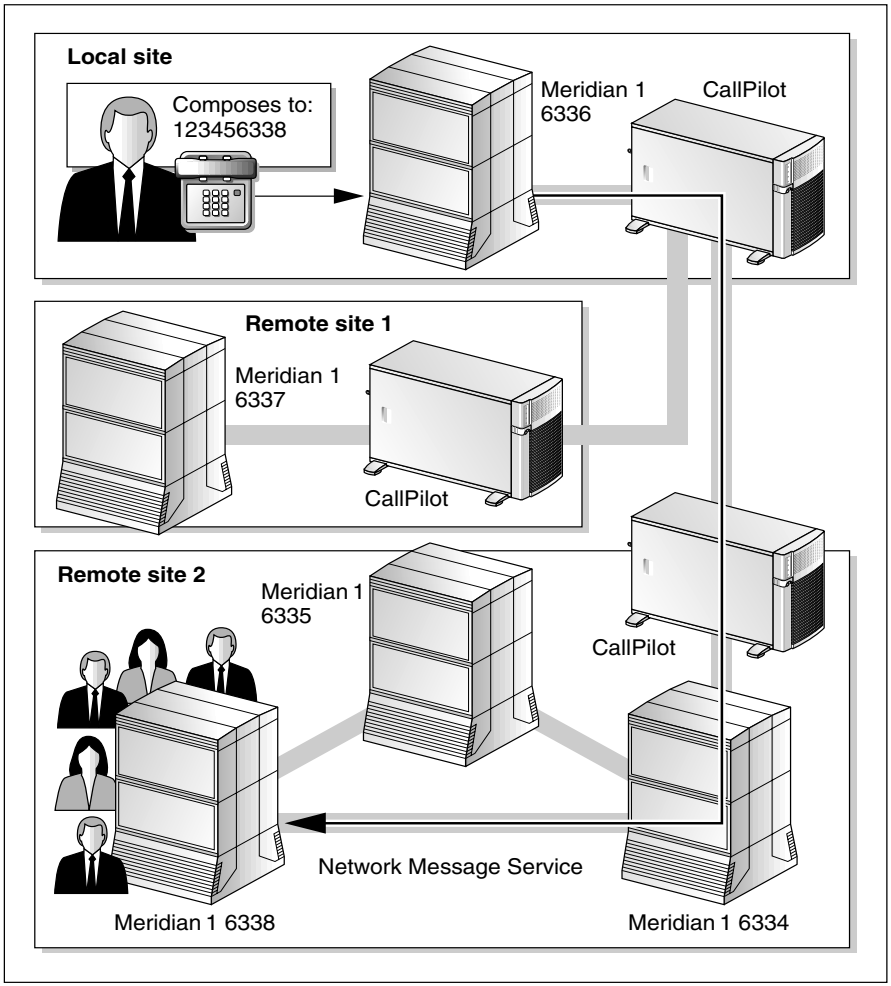
Broadcast sent to an NMS location at the local site

In the following illustration, the CallPilot system provides messaging services to four Meridian 1 switches at the local site. All users who are connected to these switches have mailboxes on the CallPilot system. The location-specific broadcast is targeted to only the users whose phonesets reside at the switch location identified by the 6338 location prefix:



Broadcast sent to an NMS location at a remote site

In the following illustration, the CallPilot system at remote site 2 provides messaging services to users on three Meridian 1 switches. The location-specific broadcast is addressed by a user on the local CallPilot system to only the users whose phonesets reside at the switch location identified by the 6338 location prefix:



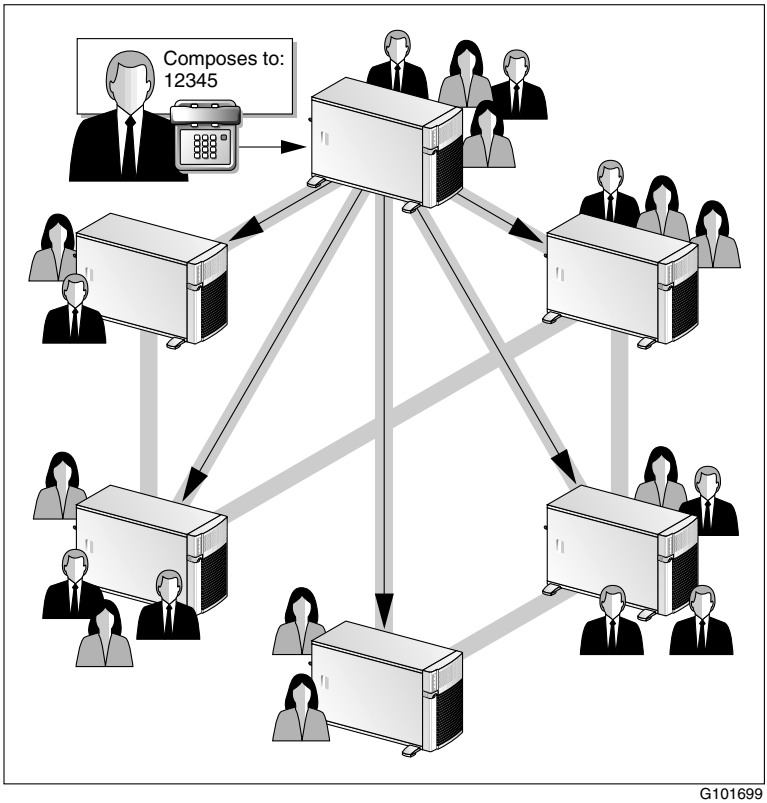
G101702

Note: If the local user wants to send a broadcast message to all NMS locations associated with a remote site, the user must address the message to each location. To simplify this task, the user can create a personal distribution list containing the location-specific broadcast address for each location.

Network broadcast

When a user sends a network-wide broadcast, the message is delivered to all users at both local and remote sites. This is accomplished by addressing the message to the network broadcast prefix.

In the following diagram, 12345 is the network broadcast prefix:



Broadcast message addresses

Introduction

The following table shows the types of broadcasts and how they are addressed.

Note: For completeness, local broadcast is also shown, even though functionality is unchanged from previous CallPilot releases.

Broadcast type	Address	Example
Local broadcast	Broadcast mailbox	5555
Network-wide broadcast	Network broadcast prefix	12345
Location-specific broadcast	Network broadcast prefix + Location prefix	12345+6338

Broadcast address rules

Network broadcast prefix

The network broadcast prefix must be between 5 and 18 digits long. The minimum length helps prevent users from accidentally composing network-wide broadcast messages.

The network broadcast prefix cannot conflict with any other prefix defined on the system. This includes, but is not limited to, the following:

- Open AMIS Compose Prefix
- Open VPIM Compose Prefix
- Delivery to Telephone (DTT) and Delivery to Fax (DTF) prefixes

- Name Dialing and Name Addressing prefixes
- network prefixes (ESN, CDP, and mailbox prefixes)

Location prefix

The location prefix is the portion of the telephone number that the user must dial to reach a user at a specific location. For example, if your dialing plan is ESN, the location prefix consists of the ESN access code used to make outgoing calls from your location (for example, 6), and the location code for the remote location (for example, 338).

For more information about dialing plans, refer to your switch documentation.

User capabilities for broadcast messages

Introduction

To send a broadcast message, the user must have the appropriate mailbox capability. If CallPilot is configured to use authentication, and the user is a desktop or web messaging user, SMTP authentication must be successful before the broadcast message is sent to the remote destinations.

Mailbox capabilities

Each user must have one of the following capabilities in the mailbox class:

Broadcast capability	Description
Local broadcast only	The user can send broadcast messages to users at ■ the local site ■ a specific NMS location associated with the local site (if Network Message Service has been installed)
Local and network broadcasts	The user can send broadcast messages to users at ■ the local site (local broadcast) ■ a specific remote site (location-specific broadcast) ■ a specific NMS location associated with either the local or a remote site (if Network Message Service has been installed; location-specific broadcast) ■ all sites in the network (network-wide broadcast)

Broadcast capability	Description
Disabled	The user cannot send any type of broadcast message.

Note: If Networking is not installed, the only options available for broadcast capability are enabled and disabled. When broadcast capability is enabled on a site that does not have networking installed, local broadcast capability is provided.

Distribution lists

Shared distribution lists

Broadcast addresses cannot be added to shared distribution lists (SDLs).

Personal distribution lists

Users can include broadcast addresses in their personal distribution lists (PDLs) according to their mailbox capability. If a user without broadcast capability attempts to add a broadcast address to his or her PDL, CallPilot informs the user that the address does not exist.

If a user wants to send a broadcast message to two or more NMS locations that are associated with a remote site, the user must address the message to each location, because each location has its own location prefix in the dialing plan. To simplify this task, the user can create a personal distribution list containing the location-specific broadcast address for each location.

Mailbox class validation for phoneset users

For phoneset users, the mailbox class includes an option to “send messages via DTT if mailbox not found.” This option determines the type of system prompt that a user without broadcast capability hears when attempting to address a broadcast message. The user may hear one of the following prompts:

- “Phone number <string entered by user>.”

- "There is no mailbox at <string entered by user>."

For security reasons, the prompt does not state that the address is a broadcast address or that the user does not have permission to send the broadcast message. Indication that the address is a broadcast address is valuable information for a hacker.

Mailbox class validation for desktop and web messaging users

The desktop or web messaging client cannot validate a user's mailbox class while sending a message. The message must be sent from the user's desktop to the CallPilot server before mailbox class validation can occur. If CallPilot determines that the user is not allowed to send the broadcast message, the user receives a non-delivery notification (NDN).

For security reasons, the NDN states that the address was not found. It does not state that the user did not have permission to send the broadcast message or suggest that the address is a broadcast address. Indication that the address is a broadcast address would be valuable information for a hacker.

SMTP authentication

To send a location-specific or network-wide broadcast message, a desktop or web messaging user must have the appropriate mailbox capability and be successfully SMTP-authenticated. If SMTP authentication fails while sending the message, the user receives an error message.

Note: For more information about SMTP authentication, see Chapter 4, "SMTP security."

CallPilot server capabilities for broadcast messages

Introduction

If Networking is installed on your CallPilot server, then users can send and receive both network-wide and location-specific broadcast messages, if broadcast capabilities are granted at both the user mailbox and CallPilot server level.

If only Network Message Service is installed on your CallPilot server, then users can send only local and location-specific broadcast messages, if broadcast capabilities are granted at the user mailbox level. Location-specific broadcast messages can be sent to any prime or satellite switch location in the local NMS network.

Levels of control

By default, broadcast capabilities at the CallPilot server level are enabled for VPIM and Enterprise Networking. If the networking protocol between the local and remote site is AMIS Networking, broadcast capability is not available because network-wide broadcast and location-specific broadcast are not supported by the AMIS protocol.

You can disable the exchange of broadcast messages between the local CallPilot server and remote voice messaging systems. When you disable the exchange of broadcast messages on the local server, you can quickly and temporarily turn off broadcasts without modifying other CallPilot settings.

You can control the exchange of broadcast messages in the local CallPilot networking database under Messaging → Message Network Configuration, as follows:

Where	How
On the local CallPilot server	Enable the following options, as required: ■ Send network broadcasts ■ Receive network broadcasts Both settings apply to the following broadcasts: ■ network-wide broadcasts ■ location-specific broadcasts to and from all locations associated with remote sites **Note:** Location-specific broadcasts to local locations are exempt because these types of broadcast messages are not actually sent over the network.
For each remote server that is defined in the network database	Enable the following options, as required: ■ Send network broadcasts to this server ■ Receive network broadcasts from this server Both settings apply to the following broadcasts: ■ network-wide broadcasts ■ location-specific broadcasts to and from this remote site ■ location-specific broadcasts to and from locations associated with this remote site

When to disable broadcast messages between sites

Use the following guidelines to determine when you should disable broadcast messages between the local and one or more remote servers:

Disable broadcast messages	when
to the local server	■ you observe a security breach, such as a hacker attempting to send messages to the local server. ■ you do not want to receive broadcast messages from remote servers.
from the local server	all users should not be allowed to send broadcast messages to other sites. For example, a small sales office may not be permitted to send network broadcast messages, whereas the corporate head office site can do so.
to a remote server	■ the remote server does not support network-wide and location-specific broadcasts. For more details, see “Broadcast messages in a mixed messaging network” on page 142. ■ the remote server does not want to receive broadcast messages from the local server.
from a remote server	■ you observe a security breach, such as a hacker attempting to send messages to the local server while pretending to be at the remote server. ■ you do not want to receive broadcast messages from the remote server.

Note: Another reason to disable broadcast messages is when you want to prevent high usage of network and CallPilot resources (network traffic, channel usage, and CPU resource usage).

See also

SMTP authentication can also restrict network broadcast messages from remote servers that are not required to authenticate before transmitting messages to the local CallPilot server. For more details, see "Unauthenticated mode" on page 84.

Broadcast messages in a mixed messaging network

Introduction

If your messaging network contains a mixture of voice messaging systems, this may affect the ability for users to send network-wide and location-specific broadcast messages to other locations.

The type of content that a broadcast message can contain (voice, fax, or text) is affected by

- the networking protocol used between two servers
- the networking solutions installed on your server
- whether the receiving server supports the content

Broadcast support between systems

The following table identifies whether network-wide and location-specific broadcast is supported on a specific type and release of voice messaging system:

Messaging system type	Network-wide broadcast	Location-specific broadcast
CallPilot 2.0	yes	yes
CallPilot 1.0x	no	no
■ Meridian Mail 12 ■ Meridian Mail 13	yes	yes
Meridian Mail 11	yes	no

Messaging system type	Network-wide broadcast	Location-specific broadcast
Meridian Mail 11 and later *with* Meridian Mail Net Gateway	yes	no
Meridian Mail 10 and earlier	no	no
Norstar VoiceMail	no	no
Business Communications Manager 2.5	no	no
Voice messaging systems from other vendors	no	no

The type of network broadcast supported between two specific servers is the lowest common denominator of what both servers support. For example, only network-wide broadcast is supported between CallPilot 2.0 and Meridian Mail 11.

Multimedia support between systems

All types of broadcast messages can contain voice, fax, or text. However, to successfully arrive at their destinations, the following requirements apply:

- The networking protocol used to send the broadcast message must support the transmission of the content.
- The remote server must support the receipt of the content.

Example 1: VPIM Networking

VPIM Networking supports the transmission of voice, fax, and text messages. Therefore, broadcast messages can contain voice, fax, or text. However, if the receiving server does not support the content, a non-delivery notification may be returned to the sender.

Example 2: Enterprise Networking

Enterprise Networking supports the transmission of voice content only. Therefore, if a user composes a broadcast message containing fax or text, and the message is to be transmitted using the Enterprise Networking protocol, the message is rejected and the sender receives a non-delivery notification.

Example 3: AMIS Networking

AMIS Networking does not support network broadcast messages.

Broadcast message content policy

You should establish a policy for the type of content that users can include in a network broadcast message, and communicate this policy to your users. You can partially enforce the policy by granting desktop messaging and fax capability in each user's mailbox class.

Configuring CallPilot for broadcast messages

Introduction

This section identifies the tasks that you must complete so that users can send location-specific and network-wide broadcast messages.

To configure CallPilot to allow broadcast messages

Note: For more detailed instructions, refer to the CallPilot Manager online Help.

1 Enable user broadcast capability in each mailbox class, as required.

In CallPilot Manager, click User → Mailbox Classes.

2 Define the network broadcast prefix.

Note: Perform this task only if the messaging network contains sites that support network broadcasts.

In CallPilot Manager, click Messaging → Messaging Management.

3 Enable CallPilot to send and receive network broadcast messages to and from all sites in the network.

In CallPilot Manager, click Messaging → Message Network Configuration → Local Server page.

4 Enable CallPilot to send and receive network broadcast messages to and from each remote server.

In CallPilot Manager, click Messaging → Message Network Configuration → Remote Server page.

ATTENTION

Ensure that the remote servers support network broadcast messages. For more information, see “Broadcast messages in a mixed messaging network” on page 142.

5 Repeat step 4 for each remote server that is defined in the network database.

Viewing or printing all broadcast addresses

Introduction

To compose broadcast messages and ensure they arrive at the correct destination, users must know the broadcast addresses. It is relatively simple to remember the local broadcast mailbox and network broadcast prefix because there are only two numbers to memorize.

However, it becomes more complex for location-specific broadcast messages, because each site or NMS location in the network database has its own location prefix.

Viewing the broadcast addresses used by each switch location

Location-specific addresses can vary depending on the location from which the broadcast message is composed. The Print Broadcast Addresses page in CallPilot Manager contains a list box that lists all local switch locations. By default, the list is shown from the local prime location's point of view. To view the broadcast addresses from a particular local satellite location's point of view, you choose the satellite location from the list box.

Note: The Print Broadcast Addresses page also shows, for your reference, the local broadcast mailbox and network broadcast prefix used by the local server.

To view or print the list of broadcast addresses

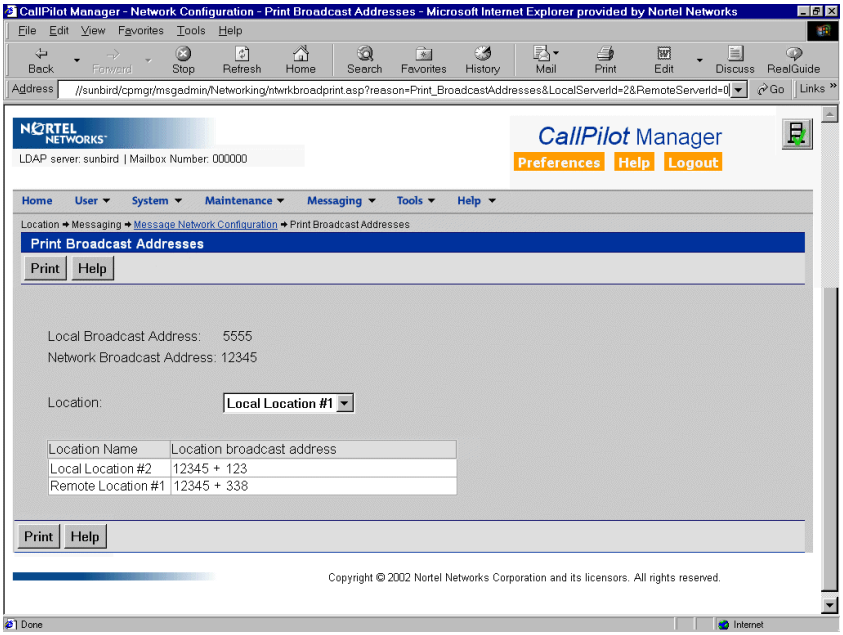
1 In CallPilot Manager, click Messaging → Messaging Network Configuration.

2 Click Print Broadcast Addresses.

Result: The Print Broadcast Addresses page appears, listing the following:

- local broadcast address
- network broadcast address
- location broadcast address for each switch location in the messaging network

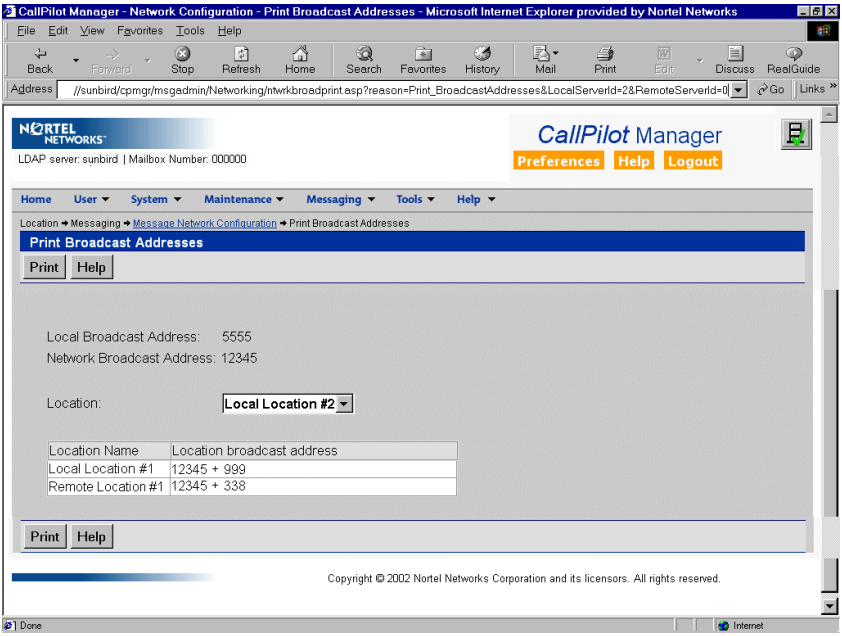
Users at the local prime switch location must use these addresses when they want to send broadcast messages to specific switch locations.



3 In the Location list box, choose the switch location for which you want to view location broadcast addresses.

Note: The list box lists only the switch locations that are associated with the local server.

Result: The Print Broadcast Addresses page refreshes with the location broadcast addresses that users at the selected switch location must use when they want to send broadcast messages to other switch locations.



4 To print the broadcast addresses, click Print.

Result: A new browser window opens, with the broadcast address list in a format suitable for printing.

5 Click File → Print.

Result: The Print dialog box opens.

6 Specify the printing options as required, and then click OK.

Result: The list is printed on your printer.

Chapter 7

Network Message Service time zone conversions

In this chapter

Overview

Introduction

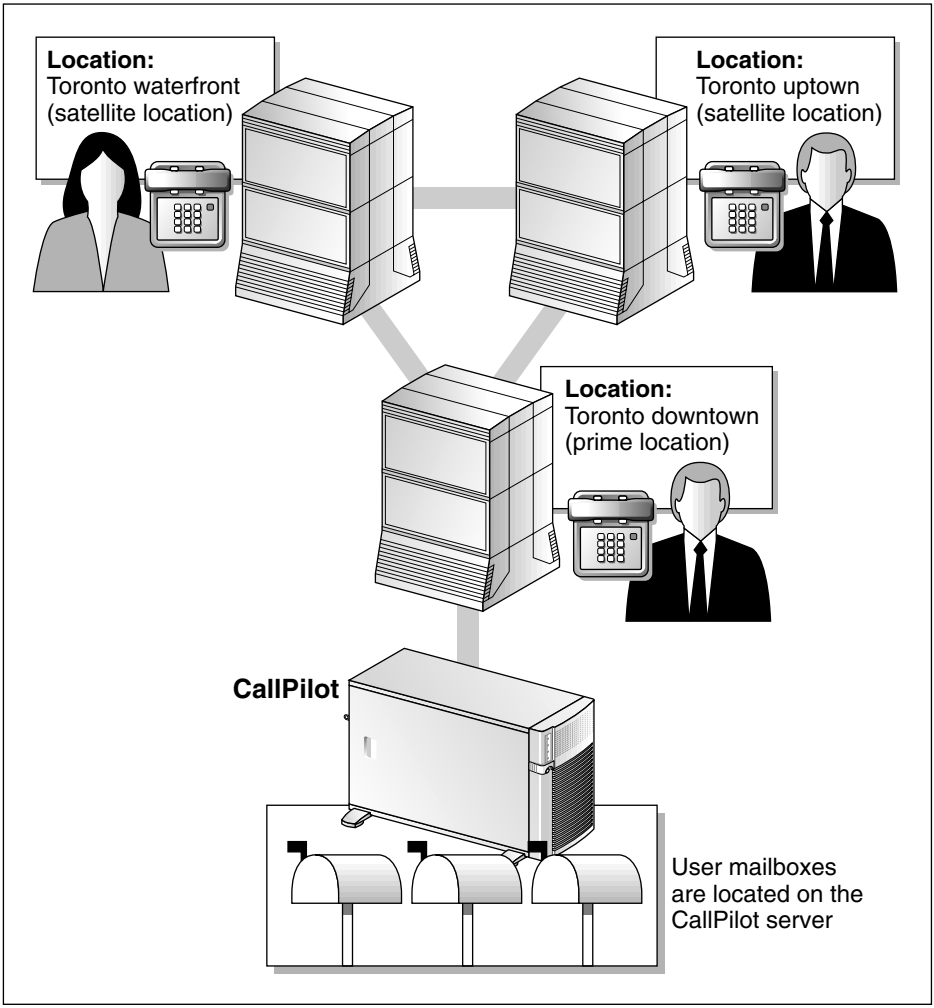
If Network Message Service is installed on your CallPilot server, and you have switch locations that are in different time zones from the CallPilot server, you can define for each switch location, the time zone in which the switch is located. This results in time and date stamps on messages and voice prompts to be indicated in the mailbox owner's time zone, instead of in the time zone of the CallPilot server.

Network Message Service description

The Network Message Service (NMS) feature in CallPilot enables your CallPilot system to provide voice messaging services to mailbox owners who reside at different switches.

In the diagram on the next page, CallPilot provides services to mailbox owners at three different switch locations in Toronto. This setup is more cost-effective than installing and running a CallPilot system at each switch location.

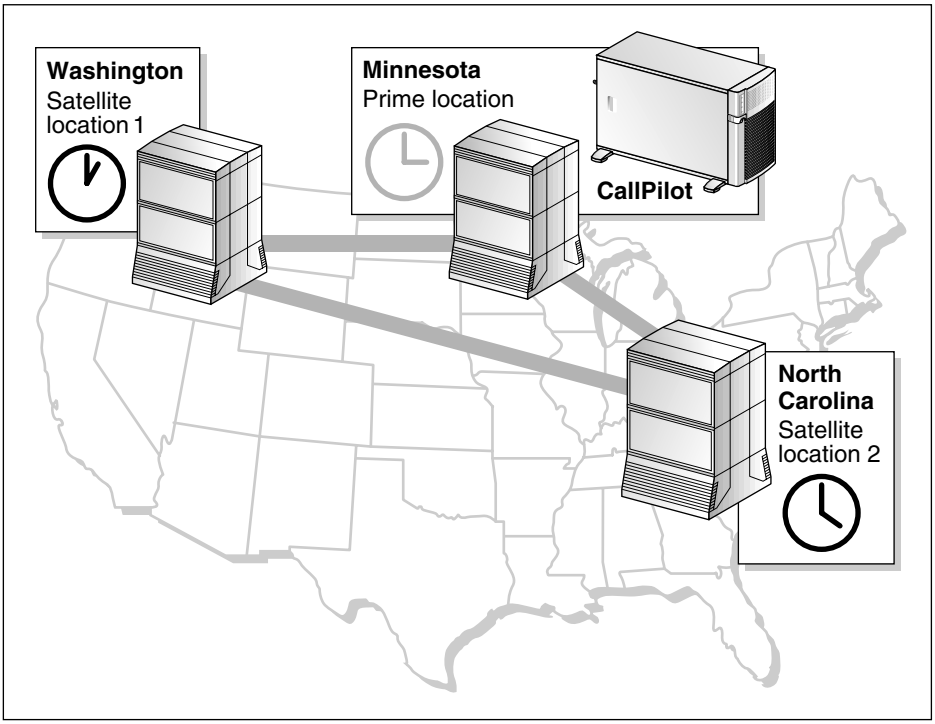
Each switch is defined in the CallPilot network database as a switch location that is associated with the CallPilot site. The switch that is directly connected to CallPilot is defined as the prime switch location. All other switches are defined as satellite switch locations.


Location:
Toronto waterfront
(satellite location)
Location:
Toronto uptown
(satellite location)
Location:
Toronto downtown
(prime location)
CallPilot
User mailboxes
are located on the
CallPilot server

G101703

Network Message Service operation in multiple time zones

In the previous illustration, all switches are located in the same time zone. Network Message Service also supports mailbox owners residing on switches in different time zones, as shown in the following diagram:



Prior to CallPilot 2.0, time and date stamps on messages and voice prompts were indicated in the CallPilot server's time zone, without the time zone name. For mailbox owners in time zones to the west of the CallPilot server, time and date stamps could potentially be in the future.

Example

A mailbox owner on the CallPilot server in Minnesota sends a local broadcast message to mailbox owners at satellite switch location 1 in Washington and satellite switch location 2 in North Carolina at 3:00 p.m. Central Time. In Washington, the current time is 1:00 p.m. Pacific Time. In North Carolina, the current time is 4:00 p.m. Eastern Time. However, the time and date stamp of the message is indicated to all mailbox owners as 3:00 p.m. The time zone is not identified.

CallPilot 2.0 time zone conversion

When Network Message Service is used in CallPilot 2.0, all time and date stamps can be presented to the mailbox owner in his or her switch location's time zone. This is accomplished by specifying the time zone for each local satellite switch location in the network database. The time zone setting can be set to one of the following:

- CallPilot server's time zone
- switch location's time zone (that is, the satellite switch location's time zone is different from the CallPilot server's time zone)

Note: The local prime location automatically acquires its time zone setting from the CallPilot server. On the CallPilot server, the time zone setting is defined in the Control Panel (which is defined when the Configuration Wizard is run).

In the example described previously, this means that the message's time and date stamp is indicated as 1:00 p.m. to the Washington mailbox owner and 4:00 p.m. to the North Carolina mailbox owner. Since the time stamp is converted to the mailbox owner's time zone, the time zone name is not required in the time and date stamp.

How time zone conversion affects mailbox owners and administrators

Phoneset users

Phoneset users benefit the most from the time zone conversion feature. All time and date stamps are converted to the time in the phoneset user's time zone.

Desktop messaging users

There is little impact to desktop messaging users since most desktop messaging clients already convert time and date stamps to the time zone configured on the PC used to access CallPilot messages. The PC must be configured with the correct time zone setting in the Date/Time component of the Windows Control Panel.

Exception: Non-delivery notifications and acknowledgments received by desktop messaging users contain a CallPilot server-generated time and date stamp in the CallPilot server's time zone, with the time zone name.

Web messaging users

For web messaging users, time and date stamps are presented in the time zone configured on the CallPilot server for the switch location at which the users reside.

CallPilot administrators

Many configuration and administration pages in CallPilot Manager contain a time field that applies to the item being configured or viewed. When Network Message Service is installed, these pages also contain a read-only time zone name field.

In some situations, an administrator can define whether the time should be presented to administrators in the server's time zone, or in the mailbox owner's time zone. The options are available only when Network Message Service is installed, and applies to the following:

- User Properties and User Creation:
  - Remote Notification

- Security
- Status (for Temporary Absence Greeting expiry)

- Message Network Configuration for the local satellite switch location

  For more details, see "Configuring the time zone for each switch location" on page 158.

How time zone conversion affects networking recipients

VPIM Networking recipients

VPIM Networking recipients are not affected since time zone information is included during transmission of VPIM Networking messages. Time and date stamps on VPIM Networking messages include the time zone name.

AMIS Networking recipients

The AMIS Networking protocol does not support the inclusion of time information in messages during transmission. The sent and received time and date stamps are always set to the time when the message is received, which is, therefore, presented in the mailbox owner's time zone.

Enterprise Networking recipients

How Enterprise Networking recipients are affected depends on whether the sending and receiving CallPilot systems are Release 2.0 or later.

Enterprise Networking cannot send or receive time zone information if the messaging server is running a release prior to CallPilot 2.0. Therefore, the time zone feature affects only the messages that are transmitted between systems that are running CallPilot Release 2.0 or later.

Configuring the time zone for each switch location

Introduction

This section identifies the tasks that you must complete so that time and date stamps are converted to the appropriate time zone for mailbox owners who reside on switches in different time zones from the CallPilot server.

Configuration overview

1. Define the time zone for the local prime switch location (see page 159).

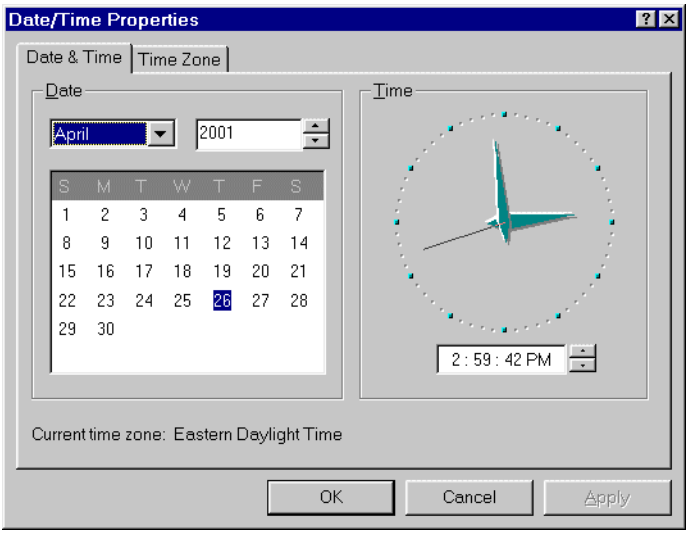
   Note: The time zone for the local prime switch location is automatically the same as the time zone for the CallPilot server. This is configured in the Date/Time component of the Windows NT Control Panel.

2. Define the time zone settings for each local satellite switch location (see page 161).

To configure the time zone for the local prime switch location

1. In Windows NT, click Start → Settings → Control Panel.
2. Double-click the Date/Time component.

   Result: The Date/Time Properties dialog box appears.



3 Click the Time Zone tab.

Result: The Time Zone page appears.

4 Ensure that the time zone selected in the list box is correct.

If it is incorrect, choose the correct time zone.

5 If required, click the check box to enable “Automatically adjust clock for daylight saving changes.”

6 Click Apply.

7 Click OK to close the Date/Time Properties dialog box.

8 Close the Control Panel.

9 Restart the server.

Result: The time zone settings in CallPilot and the Control Panel are synchronized.

To configure the time zone for each local satellite switch location

ATTENTION

Ensure that the time zone on the CallPilot server is correct before proceeding.

If the time zone on the CallPilot server is not correct and the satellite switch location is configured to use the server's time zone, time and date stamps on messages and voice prompts are incorrect. You can quickly verify the time zone setting by reviewing the local prime switch location's configuration. If it is not correct, reconfigure the time zone setting in the CallPilot server's Control Panel, then restart the server.

1 Click Messaging → Message Network Configuration.

Result: The Network Administration page appears.

2 In the Local Server Maintenance tree, click the satellite switch location you want to modify, and then click Show Details.

Result: The Satellite Location Properties page appears.

3 Do one of the following:

IF mailbox owners at this switch location are	THEN
in the same time zone as the CallPilot server	click the Use server time zone check box.
not in the same time zone as the CallPilot server	**a.** Ensure the Use server time zone check box is cleared. **b.** Select the applicable time zone from the list box.

3 Click Save.

Appendix A

Implementation and planning tools

In this chapter

Overview

Introduction

This section provides checklists and worksheets that you can use while setting up your messaging network.

Implementation checklists

To help you track your progress while implementing one or more networking solutions, you can use the following implementation checklists:

Checklist	For an example, see
AMIS Networking Implementation Checklist (NWP-035)	page 168.
Integrated AMIS Networking Implementation Checklist (NWP-032)	page 171.
Enterprise Networking Implementation Checklist (NWP-031)	page 174.
VPIM Networking Implementation Checklist (NWP-029)	page 177.
Open VPIM Implementation Checklist (NWP-036)	page 180.

For instructions on completing the tasks on these checklists, refer to the following:

- this guide
- CallPilot Manager online Help
- CallPilot 1.0 networking guides (see "Networking guides" on page 22)
- *CallPilot Administrator's Guide* (NTP 555-7101-301)

Implementation process

The implementation process is easier if you follow this recommended order:

1. Network Message Service (NMS)
   For more information, refer to the CallPilot 1.0 *NMS Implementation and Administration Guide* (NTP 555-7101-302).
2. desktop or web messaging
   For more information, refer to the *Desktop Messaging and My CallPilot Installation Guide* (NTP 555-7101-505). For information about IMAP implementation, refer to the *Desktop Messaging and My CallPilot Administration Guide* (NTP 555-7101-503).
3. AMIS Networking, Integrated AMIS Networking, Enterprise Networking or VPIM Networking
   For more information, refer to the CallPilot 1.0 networking guides listed in "Networking guides" on page 22.

Notes:

- Nortel Networks recommends that you implement and test all NMS sites in the messaging network before you implement any other networking solution.
- Nortel Networks also recommends that you verify the accuracy of information for your site before you release it to remote network administrators.

Configuration worksheets

To help you plan the configuration of your messaging network, you can use the following configuration worksheets:

Worksheet	For an example, see
Messaging Network Configuration worksheets	
CallPilot Networking—CDP Steering Codes (NWP-027)	page 184.

Worksheet	For an example, see
CallPilot Networking—ESN Location Codes (NWP-037)	page 186.
CallPilot Network Information—Local Server Maintenance (NWP-024)	page 188.
CallPilot Network Information—Remote Server Maintenance (NWP-025)	page 190.
CallPilot Network Information—Switch Location Maintenance (NWP-026)	page 192.
Messaging Delivery Configuration worksheets	
CallPilot Networking—Message Delivery Configuration (NWP-028)	page 195.
CallPilot Networking—Open VPIM Shortcuts (NWP-038)	page 199.

The configuration worksheets

- provide a hard copy record of your network
- help you capture all the information for entry into CallPilot Manager

You can send the completed worksheets to other messaging network administrators to help them configure the network databases at their sites.

Section A: Implementation checklists

In this section

AMIS Networking Implementation Checklist

Step	Description	Done
Gather information for the network		
1	Obtain the system access number for each open AMIS site with which CallPilot exchanges messages.	❒
Configure the switch **Note:** For the switch requirements, refer to the *CallPilot 1.0 AMIS Networking Implementation and Administration Guide* (NTP 555-7101-303). For instructions on configuring the switch, refer to your switch documentation.		
2	Define the ACD queues.	❒
3	Dedicate ACD agents to networking, if required.	❒
4	Verify TGAR and NCOS on ACD agents.	❒
5	Define trunks (if additional trunks are required).	❒
6	Verify access to trunks (TGAR).	❒
Configure the network database in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
7	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒
8	Configure the prime location for the local server. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
9	Configure the Network Message Service (NMS) satellite locations for the local server, if required. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒

AMIS Networking Implementation Checklist

Step	Description	Done
Configure the AMIS Networking message delivery options in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
10	Enable AMIS Networking message transmissions to and from open AMIS sites.	❒
11	Define the open AMIS compose prefix.	❒
12	Configure the AMIS Networking batch delivery threshold.	❒
13	Define the allowed open AMIS delivery times.	❒
14	Configure the local server's system access number.	❒
Configure the System and Messaging options in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
15	Define the AMIS Networking DN in the Service Directory Number (SDN) table and, if required, dedicate channels. **Note:** For guidelines on channel allocation, refer to the *CallPilot 1.0 AMIS Networking Implementation and Administration Guide* (NTP 555-7101-303).	❒
16	Define Dialing Information and Dialing Translations.	❒
Test the network for correct operation		
Note: For instructions, refer to the *CallPilot 1.0 AMIS Networking Implementation and Administration Guide* (NTP 555-7101-303).		
17	Test call routing access by testing each ACD agent.	❒
18	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
19	Send a message from a mailbox on the local server to a user at an open AMIS site, if possible.	❒

AMIS Networking Implementation Checklist

Step	Description	Done
Create a backup of the network		
20	Back up CallPilot. **Note:** For instructions, refer to the *CallPilot Administrator's Guide* (NTP 555-7101-301).	❒
21	Print CallPilot network information. **Note:** For instructions, refer to "Printing networking information" in the CallPilot Manager online Help.	❒
22	Back up the switch. **Note:** For instructions, refer to your switch documentation.	❒
23	Print switch network information. **Note:** For instructions, refer to your switch documentation.	❒

Integrated AMIS Networking Implementation Checklist

Step	Description	Done
Gather information for the network		
Note: For instructions, refer to the *CallPilot 1.0 Integrated AMIS Networking Implentation and Administration Guide* (NTP 555-7101-305). If necessary, consult with a switch technician.		
1	Gather ESN information from the switch.	❒
2	Gather CDP information from the switch.	❒
3	Draw a diagram of the existing network.	❒
4	Assign a unique site ID to each site in the network.	❒
5	Analyze the information and determine if changes are required to the dialing plan configuration on the switch.	❒
Configure the switch		
Note: For the switch requirements, refer to the *CallPilot 1.0 Integrated AMIS Networking Implementation and Administration Guide* (NTP 555-7101-305). For instructions on configuring the switch, refer to your switch documentation.		
6	Define the ACD queues.	❒
7	Dedicate ACD agents to networking, if required.	❒
8	Verify TGAR and NCOS on ACD agents.	❒
9	Define trunks (if additional trunks are required).	❒
10	Verify access to trunks (TGAR).	❒
11	Modify the dialing plan configuration on the switch if required.	❒
Configure the network sites and locations in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
12	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒

Integrated AMIS Networking Implementation Checklist

Step	Description	Done
13	Configure each remote server. Use the information recorded on the “CallPilot Networking—Remote Server Maintenance” worksheet (NWP-025).	❒
14	Configure the prime location for each of the local and remote servers. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
15	Configure the Network Message Service (NMS) satellite locations for each of the local and remote servers, if required. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
16	Convert existing sites to AMIS Networking if necessary.	❒
Configure the AMIS Networking message delivery options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
17	Enable AMIS Networking message transmissions to and from AMIS sites.	❒
18	Configure the AMIS Networking batch delivery threshold.	❒
19	Define the open AMIS compose prefix (if your network also contains open AMIS sites).	❒
20	Configure the local server’s system access number.	❒
21	Define the open AMIS delivery times (if your network also contains open AMIS sites).	❒
22	Define the AMIS Networking economy delivery times.	❒
23	Define the AMIS Networking stale times.	❒
Configure the System and Messaging options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
24	Define the AMIS Networking DN in the SDN table and, if required, dedicate channels.	❒

Integrated AMIS Networking Implementation Checklist

Step	Description	Done
25	Define Dialing Information and Dialing Translations.	❒
Test the network for correct operation		
Note: For instructions, refer to the *CallPilot 1.0 Integrated AMIS Networking Implentation and Administration Guide* (NTP 555-7101-305).		
26	Test call routing access by testing each ACD agent.	❒
27	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
28	Send a message from a mailbox on the local server to the loopback mailbox at an integrated AMIS (remote) site.	❒
29	Send a message from a mailbox on the local server to a user at an integrated AMIS (remote) site.	❒
Create a backup of the network		
30	Back up CallPilot. **Note:** For instructions, refer to the *CallPilot Administrator's Guide* (NTP 555-7101-301).	❒
31	Print CallPilot network information. **Note:** For instructions, refer to "Printing networking information" in the CallPilot Manager online Help.	❒
32	Back up the switch. **Note:** For instructions, refer to your switch documentation.	❒
33	Print switch network information. **Note:** For instructions, refer to your switch documentation.	❒

Enterprise Networking Implementation Checklist

Step	Description	Done
Gather information for the network		
Note: For instructions, refer to the *CallPilot 1.0 Enterprise Networking Implentation and Administration Guide* (NTP 555-7101-304). If necessary, consult with a switch technician.		
1	Gather ESN information from the switch.	❒
2	Gather CDP information from the switch.	❒
3	Draw a diagram of the existing network.	❒
4	Assign a unique site ID to each site in the network.	❒
5	Analyze the information and determine if changes are required to the dialing plan configuration on the switch.	❒
Configure the switch		
Note: For the switch requirements, refer to the *CallPilot 1.0 Enterprise Networking Implementation and Administration Guide* (NTP 555-7101-304). For instructions on configuring the switch, refer to your switch documentation.		
6	Define the ACD queues.	❒
7	Dedicate ACD agents to networking (if required). This step is optional.	❒
8	Verify TGAR and NCOS on ACD agents.	❒
9	Define trunks (if additional trunks are required).	❒
10	Verify access to trunks (TGAR).	❒
11	Modify the dialing plan configuration on the switch if required.	❒
Configure the network sites and locations in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
12	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒

Enterprise Networking Implementation Checklist

Step	Description	Done
13	Configure each remote server. Use the information recorded on the “CallPilot Networking—Remote Server Maintenance” worksheet (NWP-025).	❒
14	Configure the prime location for each of the local and remote servers. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
15	Configure the Network Message Service (NMS) satellite locations for each of the local and remote servers (if required). Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
16	Convert existing sites to Enterprise Networking if necessary.	❒
Configure the Enterprise Networking message delivery options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
17	Enable Enterprise Networking message transmissions to and from Enterprise Networking sites.	❒
18	Configure the Enterprise Networking batch delivery threshold.	❒
19	Define the Enterprise Networking economy delivery times.	❒
20	Define the Enterprise Networking stale times.	❒
Configure the System options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
21	Define the Enterprise Networking DN in the Service Directory Number (SDN) table and, if required, dedicate channels.	❒
Test the network for correct operation **Note:** For instructions, refer to the *CallPilot 1.0 Enterprise Networking Implentation and Administration Guide* (NTP 555-7101-304).		
22	Test call routing access by testing each ACD agent.	❒

Enterprise Networking Implementation Checklist

Step	Description	Done
23	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
24	Send a message from a mailbox on the local server to the loopback mailbox at a remote Enterprise Networking site.	❒
25	Send a message from a mailbox on the local server to a mailbox user at a remote Enterprise Networking site.	❒
Create a backup of the network		
26	Back up CallPilot. **Note:** For instructions, refer to the *CallPilot Administrator's Guide* (NTP 555-7101-301).	❒
27	Print CallPilot network information. **Note:** For instructions, refer to "Printing networking information" in the CallPilot Manager online Help.	❒
28	Back up the switch. **Note:** For instructions, refer to your switch documentation.	❒
29	Print switch network information. **Note:** For instructions, refer to your switch documentation.	❒

VPIM Networking Implementation Checklist

Step	Description	Done
Gather information for the network		
1	Obtain the following information for each remote server: — fully qualified domain name (FQDN) — VPIM prefix for each switch location at the remote site — SMTP password (if SMTP authentication is being used)	❒
2	Obtain the fully qualified domain name of the outgoing SMTP mail/proxy server.	❒
3	Draw a diagram of the existing network.	❒
4	Assign a unique site ID to each site in the network.	❒
5	Create a VPIM network shortcut for each switch location in the network (for both the local and remote servers).	❒
Configure the network sites and locations in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
6	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒
7	Configure each remote server. Use the information recorded on the “CallPilot Networking—Remote Server Maintenance” worksheet (NWP-025).	❒
8	Configure the prime location for each of the local and remote servers. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
9	Configure the Network Message Service (NMS) satellite locations for each of the local and remote servers (if required). Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
10	Convert existing sites to VPIM Networking if necessary.	❒

VPIM Networking Implementation Checklist

Step	Description	Done
Configure the VPIM Networking message delivery options in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
11	Enable incoming SMTP/VPIM message transmissions from desktop or web messaging users and open VPIM sites.	❒
12	Enable outgoing VPIM Networking message transmissions to open VPIM sites.	❒
13	Configure the Outgoing SMTP mail/proxy server's FQDN.	❒
14	Define the open VPIM compose prefix (if required).	❒
15	Create an open VPIM shortcut for each open VPIM-compliant site with which CallPilot exchanges messages (if required).	❒
16	Configure the encryption settings (if required).	❒
17	Configure the SMTP authentication settings (if required).	❒
18	Configure the unauthenticated access restrictions for users and remote servers, if users or servers in your network will not be SMTP authenticated.	❒
Test the network for correct operation		
Note: For instructions, refer to the *CallPilot 1.0 VPIM Networking Implentation and Administration Guide* (NTP 555-7101-306).		
19	Perform a connectivity test by pinging the outgoing SMTP mail/proxy server or by establishing a telnet connection to the server.	❒
20	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
21	Send a message from a mailbox on the local server to a mailbox user at a remote VPIM Networking site.	❒

VPIM Networking Implementation Checklist

Step	Description	Done
Create a backup of the network		
22	Back up CallPilot. **Note:** For instructions, refer to the *CallPilot Administrator's Guide* (NTP 555-7101-301).	❒
23	Print CallPilot network information. **Note:** For instructions, refer to "Printing networking information" in the CallPilot Manager online Help.	❒

Open VPIM Implementation Checklist

Step	Description	Done
Gather information for the network		
1	Obtain the following for each open VPIM-compliant site with which CallPilot exchanges messages: — fully qualified domain name — VPIM prefix	❒
2	Obtain the fully qualified domain name of the outgoing SMTP mail/proxy server.	❒
3	Draw a diagram of the existing network.	❒
4	Create an open VPIM shortcut for each open VPIM site.	❒
Configure the network database in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
5	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒
6	Configure the prime location for the local server. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
7	Configure the Network Message Service (NMS) satellite locations for the local server, if required. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
Configure the VPIM Networking message delivery options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
8	Enable incoming SMTP/VPIM message transmissions from desktop or web messaging users and open VPIM sites.	❒
9	Enable outgoing VPIM Networking message transmissions to open VPIM sites.	❒
10	Configure the Outgoing SMTP mail/proxy server’s FQDN.	❒

Open VPIM Implementation Checklist

Step	Description	Done
11	Define the open VPIM compose prefix.	❒
12	Create an open VPIM shortcut for each open VPIM-compliant site with which CallPilot exchanges messages, if required.	❒
13	Configure the encryption settings, if required.	❒
14	Configure the SMTP authentication settings, if required.	❒
15	Define unauthenticated access restrictions for users and remote servers, if users or servers in your network will not be SMTP authenticated.	❒
Test the network for correct operation		
Note: For instructions, refer to the *CallPilot 1.0 VPIM Networking Implentation and Administration Guide* (NTP 555-7101-306).		
16	Perform a connectivity test by pinging the outgoing SMTP mail/proxy server or by establishing a telnet connection to the server.	❒
17	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
18	Send a message from a mailbox on the local server to a mailbox user at an open VPIM site, if possible.	❒
Create a backup of the network		
19	Back up CallPilot. **Note:** For instructions, refer to the *CallPilot Administrator's Guide* (NTP 555-7101-301).	❒
20	Print CallPilot network information. **Note:** For instructions, refer to "Printing networking information" in the CallPilot Manager online Help.	❒

Section B: Configuration worksheets

In this section

CallPilot Networking—CDP Steering Codes

Complete and attach this form to NWP-024, NWP-025 or NWP-026.

Location information

This location belongs to site name:	Site ID:
Location name:	Location ID:

CDP steering codes

(You can define up to 500 steering codes for this switch location. Complete and attach additional pages, as required.)

CDP steering code:	Overlap between CDP steering code and local extensions:	CDP steering code:	Overlap between CDP steering code and local extensions:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

CallPilot Networking—CDP Steering Codes

CDP steering codes (continued)

CDP steering code:	Overlap between CDP steering code and local extensions:	CDP steering code:	Overlap between CDP steering code and local extensions:

Completed by

Administrator:	Date:

CallPilot Networking—ESN Location Codes

Complete and attach this form to NWP-024, NWP-025 or NWP-026.

Location information

This location belongs to site name:	Site ID:
Location name:	Location ID:

ESN location codes

(You can define up to 30 location codes for this switch location.)

ESN location code:	Overlap between ESN location code and local extensions:	ESN location code:	Overlap between ESN location code and local extensions:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

CallPilot Networking—ESN Location Codes

ESN location codes (continued)

ESN location code:	Overlap between ESN location code and local extensions:	ESN location code:	Overlap between ESN location code and local extensions:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Completed by

Administrator:	Date:

CallPilot Networking—Local Server Maintenance

Note: Complete and attach CallPilot Networking—Switch Location Maintenance (NWP-026) for the prime switch location.

Local server information

Site name:	Site ID:
Does site use Network Message Service? ❒ Yes ❒ No	
Send messages to all other servers: ❒ Yes ❒ No	Activate Names Across the Network (add or update remote users on this server): ❒ Yes ❒ No

Network broadcast ability

Send network broadcast messages to remote sites: ❒ Yes ❒ No	Receive network broadcast messages from remote sites: ❒ Yes ❒ No

Network broadcast addresses

Location broadcast number: Refer to the prime and satellite configuration for each location.
Network broadcast number: **Note:** Configure the network broadcast mailbox number in Messaging → Messaging Administration.

Enterprise Networking options

Receive message text information: ❒ Yes ❒ No

CallPilot Networking—Local Server Maintenance

SMTP and VPIM Networking

Local server's FQDN:

Completed by

Administrator:	Date:

CallPilot Networking—Remote Server Maintenance

Note: Complete and attach CallPilot Networking—Switch Location Maintenance (NWP-026) for the prime switch location.

Remote server information

Site name:	Does site use Network Message Service? ❒ Yes ❒ No
Server type: ❒ CallPilot ❒ MMNG ❒ Meridian Mail ❒ Norstar ❒ Other	
Site ID:	Send messages to this server: ❒ Yes ❒ No

Network broadcast ability

Send network broadcast messages to this server: ❒ Yes ❒ No	Receive network broadcast messages from this server: ❒ Yes ❒ No

Enterprise Networking options

Send local user information to this server: ❒ Yes ❒ No	Send message text information to this server: ❒ Yes ❒ No

SMTP and VPIM Networking

Remote server's FQDN:

CallPilot Networking—Remote Server Maintenance

Connection information

Message transfer protocol: ❒ AMIS ❒ Enterprise ❒ VPIM	Connection DNs (Enterprise Networking only) **Note:** If the remote server is uses the AMIS protocol, complete the "Remote system access number" section below: DN 1: _____ DN 2: _____ DN 3: _____

Remote system access number (complete one only)

Complete this section only if the remote server uses the AMIS protocol.

Public network number: Country code: _____ Area/city code: _____ Number: _____	Private network number: _____

Enterprise Networking passwords

Initiating password: _____
Responding password: _____

VPIM Networking security

SSL port number (for encryption):		
Server password:		
Receive messages from this server:	❒ Yes	❒ No

Completed by

Administrator:	Date:

NWP-025 Page 2 of 2

CallPilot Networking—Switch Location Maintenance

Complete this form for each switch location and attach it to NWP-024 or NWP-025.

Location Information

This location belongs to Site name: Site ID:	This location is a ❒ Prime switch location ❒ Satellite switch location
Location name:	Do you want to record a spoken name for the location? ❒ Yes (Click Record or import.) ❒ No
Location ID:	

Dialing plans

❒ ESN (Complete the ESN dialing plan information section below.)	❒ CDP (Complete the CDP dialing plan information section on the next page.)
Mailbox addressing follows the dialing plan: ❒ Yes ❒ No (Complete the Mailbox prefixes field.)	
Mailbox prefixes: _____ _____	Dialing prefix (for remote locations only): _____

ESN dialing plan information

(Complete this section if you have selected the ESN dialing plan.)

ESN access code:
ESN location codes and overlap: Complete and attach “ESN Location Codes” (NWP-037).

CallPilot Networking—Switch Location Maintenance

CDP dialing plan information

(Complete this section if you have selected the CDP dialing plan.)

CDP steering codes and overlap: Complete and attach “CDP Steering Codes” (NWP-027).

VPIM network shortcuts

(Complete this section to allow phoneset users to send VPIM Networking messages. You can create up to 30 VPIM network shortcuts for this location.)

VPIM prefix:	Overlap between VPIM prefix and local extensions:	VPIM prefix:	Overlap between VPIM prefix and local extensions:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

CallPilot Networking—Switch Location Maintenance

VPIM network shortcuts (continued)

VPIM prefix:	Overlap between VPIM prefix and local extensions:	VPIM prefix:	Overlap between VPIM prefix and local extensions:
_____	_____	_____	_____
_____	_____	_____	_____

Time zone

(Complete this section for local satellite switch locations only.)

Use server time zone: ❒ Yes ❒ No (Specify the time zone to be used.)	Time zone (if server time zone will not be used:

Completed by

Administrator:	Date:

CallPilot Networking—Message Delivery Configuration

AMIS Networking options

Enable outgoing AMIS Networking messages ❒ Yes ❒ No	Enable incoming AMIS Networking messages ❒ Yes ❒ No
Number of messages to collect before sending (batch threshold):	Open AMIS compose prefix:

Open AMIS Networking delivery times

Days active: ❒ Monday	❒ Tuesday	❒ Wednesday	❒ Thursday
❒ Friday	❒ Saturday	❒ Sunday	
Outgoing messages allowed on business days (hh:mm)		From: _____ To: _____	
Outgoing messages allowed on non-business days (hh:mm)		From: _____ To: _____	

Local system access number (complete one only)

Public network number: Country code: _____ Area/city code: _____ Number: _____	Private network number: _____

Economy delivery times (hh:mm)

Open AMIS Start time: _____ Stop time: _____	Integrated AMIS Start time : _____ Stop time: _____

NWP-028 Page 1 of 4

CallPilot Networking—Message Delivery Configuration

AMIS Networking options (continued)

Stale times (hh:mm)

Economy Open AMIS: _____ Economy Integrated AMIS: _____	Standard _____ Urgent: _____

Enterprise Networking options

Enable outgoing Enterprise Networking messages ❒ Yes ❒ No	Enable incoming Enterprise Networking messages ❒ Yes ❒ No
Number of messages to collect before sending (batch threshold):	

Economy delivery times (hh:mm)

Start time:	Stop time:

Stale times (hh:mm)

Economy:	Standard:
Urgent:	

SMTP and VPIM Networking options

Enable incoming VPIM Networking messages: ❒ Yes ❒ No	Enable outgoing VPIM Networking messages: ❒ Yes ❒ No
Outgoing SMTP Mail/Proxy server:	

CallPilot Networking—Message Delivery Configuration

SMTP and VPIM Networking options (continued)

Open VPIM compose prefix:
Open VPIM shortcuts: Complete and attach “Open VPIM Shortcuts” (NWP-038).

Security modes for SMTP sessions

Note: These settings apply for VPIM Networking, desktop messaging, and web messaging.

Encryption options

Enable SSL for incoming SMTP sessions:	❒ Yes	❒ No
Connect to server with SSL for Outgoing SMTP sessions:	❒ Yes	❒ No

Authentication options

Note: If you choose Yes for Unauthenticated as well as either Challenge and Response or User ID and Password authentication, this is referred to as *mixed authentication*.

Unauthenticated:	❒ Yes	❒ No
Challenge and Response authentication:	❒ Yes	❒ No
User ID and Password authentication:	❒ Yes	❒ No
SMTP/VPIM password for initiating authenticated connections to remote servers:	_____	

Authentication failure attempts

Maximum failed authentication attempts from a remote server:	_____	
Action to perform when the maximum has been reached:	❒ Log only	❒ Log and disable server
Maximum failed authentication attempts from a user:	_____	
Action to perform when the maximum has been reached:	❒ Log only	❒ Log and disable user

CallPilot Networking—Message Delivery Configuration

SMTP and VPIM Networking options (continued)

Unauthenticated access restrictions

Enable unauthenticated desktop user restrictions	❒ Yes	❒ No
Delivery to telephone or fax	❒ Yes	❒ No
Enable Open AMIS	❒ Yes	❒ No
Enable Integrated Networking	❒ Yes	❒ No
Enable SDL addressing	❒ Yes	❒ No
Enable broadcast addressing	❒ Yes	❒ No
Restrict the number of recipients		
Maximum recipients	_____	
Enable unauthenticated server restrictions:		
Enable SDL addressing	❒ Yes	❒ No
Enable broadcast addressing	❒ Yes	❒ No
Restrict the number of recipients	❒ Yes	❒ No
Maximum recipients	_____	

Remote contact options (AMIS and Enterprise Networking)

Wait before sending C DTMF tone (milliseconds):
Delay for each non-pause character in DN (milliseconds):

Completed by

Administrator:	Date:

CallPilot Networking—Open VPIM Shortcuts

Complete and attach this form to NWP-028.

Open VPIM shortcuts

(You can define up to 500 open VPIM shortcuts. Complete and attach additional pages, if required.)

VPIM prefix	FQDN (domain name)	VPIM prefix	FQDN (domain name)

Completed by

Administrator:	Date:

NWP-038 Page 1 of 1

Index

A

B

C

D

E

F

I

J

K

L

M

N

O

P

R

S

T

U

V

W

CallPilot

Networking Enhancements Guide

Publication number:	555-7101-507
Product release:	2.0
Document release:	Standard 1.0
Date:	September 2002

NORTEL NETWORKS™