

VERSION 2.5

NIMS Administration

Novell Internet Messaging System



Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 2000 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Online Documentation:

Novell Trademarks

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

eDirectory is a trademark of Novell, Inc.

GroupWise is a registered trademark of Novell, Inc. in the United States and other countries.

ManageWise is a registered trademark of Novell, Inc. in the United States and other countries.

NDS is a registered trademark of Novell, Inc. in the United States and other countries.

NLM is a trademark of Novell, Inc.

Novell Certificate Server is a trademark of Novell, Inc.

Novell Internet Messaging System is a trademark of Novell, Inc.

Novell Technical Services is a service mark of Novell, Inc.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

1	NIMS System Overview	11
----------	-----------------------------	-----------

2	Planning and Configuring Your NIMS System	35
----------	--	-----------

3 Configuring NIMS Objects and Agents

61

4 Optimizing Your NIMS Messaging Servers

115

5	Configuring Email Clients for Use with NIMS	121
6	Managing NIMS Users	127
A	NIMS Commands and Utilities	137
B	NIMS Directory Structure and Message Processing	151

C	Troubleshooting	161
D	Setting Up SSL	171
E	Sample NIMS Configurations	179
F	Supported Standards	187

1

NIMS System Overview

If you have followed the instructions in the Novell® Internet Messaging System (NIMS) *Quick Start*, you have installed a basic NIMS system. In case you haven't performed the initial installation yet, the instructions are repeated in this guide for your convenience. The additional topics listed below help you understand what takes place when you install your initial NIMS system and plan what you need to do to set up your complete NIMS system.

- ♦ “Initial NIMS Installation” on page 11
- ♦ “Initial NIMS System” on page 22
- ♦ “Standalone Configuration” on page 25
- ♦ “Distributed Configuration” on page 26
- ♦ “NIMS System Administration” on page 27

Initial NIMS Installation

This section repeats the installation information covered in the *NIMS Quick Start*. During initial installation, you set up a basic NIMS system. Select the platform on which you are installing NIMS:

- ♦ “NIMS Installation on NetWare” on page 12
- ♦ “NIMS Installation on Solaris” on page 15
- ♦ “NIMS Installation on Linux” on page 19

NIMS Installation on NetWare

- ♦ “NIMS System Requirements on NetWare” on page 12
- ♦ “NIMS Prerequisites on NetWare” on page 12
- ♦ “Installing the NIMS Software on NetWare” on page 13
- ♦ “Starting NIMS on NetWare” on page 15

NIMS System Requirements on NetWare

- ♦ NetWare® 4.11 or later
- ♦ 7 MB of disk space for installation; disk space for the NIMS message store varies based on the number of users and the amount of disk space allowed per mailbox
- ♦ 32 MB of available memory beyond normal NetWare requirements for a NIMS system of up to 50 simultaneous connections; additional connections require additional memory
- ♦ The latest Support Pack for your version of NetWare (recommended but not required); you can download the latest Support Pack from the [Novell Support Connection \(http://support.novell.com/\)](http://support.novell.com/)
- ♦ Long filename support for your version of NetWare; see your NetWare documentation for instructions

NIMS Prerequisites on NetWare

- ♦ Make sure you have Admin rights to the NDS® tree where you plan to install NIMS. You must provide the administrator username and password during installation so the installation program can extend the schema.
- ♦ Decide what you want to name the Messaging Server object. The default is *server_name* Messaging Server. Make sure you know the domain name your NIMS system will service and the IP addresses of primary and secondary DNS servers.
- ♦ Check for the possibility of duplicate port numbers on your server. Ports 80 and 389 are the default ports used by two of the NIMS agents. If other programs on the server already use those ports, conflicts will occur. To change the port numbers used by the NIMS agents, see “[Configuring the WebMail Agent](#)” on page 89 and “[Configuring the Address Book Agent](#)” on page 95.

Installing the NIMS Software on NetWare

- 1** Place the NIMS CD in the CD drive of the NetWare server where you want to install NIMS > mount the CD drive. See your NetWare documentation for instructions.
- 2** If you are upgrading from an earlier version of NIMS, unload the NIMS NLM programs and make sure no one is running NetWare Administrator before continuing.
- 3** On a NetWare 5.x server, enter **nwconfig** at the console prompt.
or
On a NetWare 4.1x server, enter **load install** at the console prompt.
- 4** From the Configuration Options menu, select Product Options > press Enter.
- 5** Select Install a Product Not Listed > press Enter.
- 6** Press F3 > delete the default path > enter the volume name of the NIMS CD. For example:

NIMS2_5:

A list of installation options appears.

- 7** If this is a new NIMS 2.5 installation, select the following:
 - ♦ First-Time Directory Install (extends the NDS schema)
 - ♦ Configure Server for NIMS (prompts you later for the Messaging Server object name, domain name, and DNS server addresses; allows you to select which NIMS agents to configure; creates the message store on the SYS: volume)

If you choose not to have the installation program configure the server for you, you must create NIMS objects manually. See [Chapter 2, “Planning and Configuring Your NIMS System,”](#) on page 35 and [Chapter 3, “Configuring NIMS Objects and Agents,”](#) on page 61.

 - ♦ Novell Internet Messaging System Files (copies the NIMS files to the server)

or

If you are upgrading from an earlier version of NIMS, select the following:

- ♦ Back Up Files from Versions 2.0, 2.01, and 2.1 (optional)

- ♦ Directory Schema Update (adds new NIMS objects to the NDS schema)
- ♦ Novell Internet Messaging System Files (copies the NIMS files to the server)

8 Press F10 to continue.

9 Enter the administrator name > enter the administrator password > repeat the password > press Esc > select Yes to continue.

10 In the Configuration Parameters dialog box, provide the following information for a new NIMS installation:

Enter the name of the Messaging Server object in NDS. By default, the Messaging Server object will be created in the Internet Services container and the message store will be created on the SYS: volume.

Enter the name of the primary domain to be serviced by your NIMS system.

Enter the IP address of one or two DNS servers that will resolve host names into IP addresses for your NIMS system.

11 Select the NIMS agents to create NDS objects for in a new NIMS installation:

The SMTP Agent is the means by which messages enter and leave your NIMS system across the Internet.

The POP Agent provides mailbox access for users with any POP3 email client.

The IMAP Agent provides mailbox access for users with any IMAP4 email client.

The WebMail Agent provides mailbox access to users' mailboxes by way of any Web browser.

Forwarding is provided by the AutoReply Agent, which also lets users set up an automated email response when they are not monitoring their mailboxes.

The Alias Agent enables your NIMS system to recognize usernames in a variety of formats.

The Finger Agent lets finger clients find out information about NIMS users.

LDAP support is provided by the Address Book Agent, which allows users to access address book information in NDS.

The AntiSpam Agent protects your NIMS system from UBE (unsolicited bulk email) or SPAM messages.

The Proxy Agent lets users consolidate messages from other POP3 and IMAP4 email accounts into their NIMS mailboxes.

For detailed information on each NIMS agent, see **Chapter 3, “Configuring NIMS Objects and Agents,”** on page 61.

- 12** Continue to follow the installation instructions on the screen until you have exited the NIMS installation program.

Starting NIMS on NetWare

On a NetWare 5.x server, enter **ims** at the console prompt. On a NetWare 4.11 server, enter **load ims** at the console prompt. You will notice that many NLM programs load when you start NIMS.

During installation, the AUTOEXEC.NCF file was updated to include the appropriate command to start NIMS automatically each time you restart your server. To stop NIMS on a NetWare 5.x server, enter **ims unload** at the console prompt. On a NetWare 4.x server, enter **load ims unload**.

Continue with **“Initial NIMS System”** on page 22.

NIMS Installation on Solaris

- ♦ **“NIMS System Requirements on Solaris”** on page 15
- ♦ **“NIMS Prerequisites on Solaris”** on page 16
- ♦ **“Installing the NIMS Software on Solaris”** on page 16
- ♦ **“Starting NIMS on Solaris”** on page 18

NIMS System Requirements on Solaris

- ♦ Sun* Solaris* 2.6 or later
- ♦ NDS for Solaris installed; see NDS for Solaris on the [Novell Software Downloads page](http://www.novell.com/download/#NDS) (<http://www.novell.com/download/#NDS>)

- ♦ 20 MB of disk space for installation; disk space for the NIMS message store varies based on the number of users and the amount of disk space allowed per mailbox

NIMS Prerequisites on Solaris

- ♦ Make sure you have Admin rights to the NDS tree where you plan to install NIMS. You must provide the administrator username and password during installation so the installation program can extend the schema.
- ♦ Decide what you want to name the Messaging Server object. The default is *server_name* Messaging Server. Make sure you know the domain name your NIMS system will service and the IP addresses of primary and secondary DNS servers.
- ♦ Check for the possibility of duplicate port numbers on your server. Ports 80 and 389 are the default ports used by two of the NIMS agents. If other programs on the server already use those ports, conflicts will occur. To change the port numbers used by the NIMS agents, see “Configuring the WebMail Agent” on page 89 and “Configuring the Address Book Agent” on page 95.
- ♦ Stop `sendmail` on the server where you will install NIMS and make sure it will not autoload when your server restarts. NIMS and `sendmail` cannot run on the same server.
- ♦ Check the `/etc/syslog.conf` file for a line that starts with `mail.debug`. If it exists, comment it out. In debug mode, mail produces enough syslog messages to fill most disks in a short period of time.

Installing the NIMS Software on Solaris

- 1 Log in as `root` > mount the NIMS CD. See your Solaris documentation for instructions.

You have several options for installing NIMS. You can install directly from the CD. You can copy the contents of the CD into a temporary directory on your Solaris server. You can FTP the contents of the CD or temporary directory to a remote server.

The files and directories you need access to during installation are the `pinstall.sol` script, the NIMS directory, and the Pervasive directory (if you have not already installed Pervasive).

- 2** Change to the directory where `pinstall.sol` is located > enter `./pinstall.sol` at the command prompt.

The `pinstall.sol` script performs the following actions:

- ♦ Verifies that NDS for Solaris has been installed
- ♦ Checks to determine if Pervasive has been installed; if not, it installs Pervasive
- ♦ Copies the NIMS files to the installation directory
- ♦ Starts the `nimsext.sh` script

- 3** Type the administrator name > press Tab > type the password > press Enter.

You might need to wait a few moments before continuing. Do not press any keys while waiting. Please be patient.

- 4** When prompted, select Add Schema Extensions > press Enter > select Configure the Server > press Enter > follow the on-screen instructions to continue.

If you choose not to have the installation program configure the server for you, you must create NIMS objects manually. See [Chapter 2, “Planning and Configuring Your NIMS System,”](#) on page 35 and [Chapter 3, “Configuring NIMS Objects and Agents,”](#) on page 61.

- 5** In the Configuration Parameters dialog box, provide the following information to configure your NIMS server, pressing Tab to move from field to field:

Enter the name of the Messaging Server object
in NDS.

Enter the name of the primary domain to be serviced
by your NIMS system.

Enter the IP address of one or
two DNS servers that will resolve host names into IP addresses for your
NIMS system.

- 6** Select the NIMS agents to create NDS objects for, pressing Tab to move from field to field and using the Spacebar to select or deselect:

The SMTP Agent is the means by which messages enter and
leave your NIMS system across the Internet.

The POP Agent provides mailbox access for users with any POP3 email client.

The IMAP Agent provides mailbox access for users with any IMAP4 email client.

The WebMail Agent provides mailbox access to users' mailboxes by way of any Web browser.

Forwarding is provided by the AutoReply Agent, which also lets users set up an automated email response when they are not monitoring their mailboxes.

The Alias Agent enables your NIMS system to recognize usernames in a variety of formats.

The Finger Agent lets finger clients find out information about NIMS users.

LDAP support is provided by the Address Book Agent, which allows users to access address book information in NDS.

The AntiSpam Agent protects your NIMS system from UBE (unsolicited bulk email) or SPAM messages.

The Proxy Agent lets users consolidate messages from other POP3 and IMAP4 email accounts into their NIMS mailboxes.

For detailed information on each NIMS agent, see [Chapter 3, "Configuring NIMS Objects and Agents,"](#) on page 61.

- 7** Continue to follow the installation instructions on the screen until you have exited the NIMS installation program.

Starting NIMS on Solaris

On Solaris, the NIMS software is installed in `/opt/NOVLnims` and its subdirectories. The NIMS startup script on Solaris is `/etc/init.d/nims`. Use the following commands to start and stop your NIMS system:

```
/etc/init.d/nims start  
/etc/init.d/nims stop
```

Continue with ["Initial NIMS System"](#) on page 22.

NIMS Installation on Linux

- ♦ “Linux System Requirements” on page 19
- ♦ “Linux Prerequisites” on page 19
- ♦ “Installing the NIMS Software on Linux” on page 20
- ♦ “Starting NIMS on Linux” on page 22

Linux System Requirements

- ♦ Red Hat* Linux* 6.0 or later (any version of Red Hat Linux supported by NDS)
- ♦ NDS for Linux installed; see eDirectory for Linux on the [Novell Software Downloads page \(http://www.novell.com/download/#NDS\)](http://www.novell.com/download/#NDS)
- ♦ 20 MB of disk space for installation; disk space for the NIMS message store varies based on the number of users and the amount of disk space allowed per mailbox

Linux Prerequisites

- ♦ Make sure you have Admin rights to the NDS tree where you plan to install NIMS. You must provide the administrator username and password during installation so the installation program can extend the schema.
- ♦ Decide what you want to name the Messaging Server object. The default is *server_name* Messaging Server. Make sure you know the domain name your NIMS system will service and the IP addresses of primary and secondary DNS servers.
- ♦ Check for the possibility of duplicate port numbers on your server. Ports 80 and 389 are the default ports used by two of the NIMS agents. If other programs on the server already use those ports, conflicts will occur. To change the port numbers used by the NIMS agents, see “[Configuring the WebMail Agent](#)” on page 89 and “[Configuring the Address Book Agent](#)” on page 95.
- ♦ Stop `sendmail` on the server where you will install NIMS and make sure it will not autoloading when your server restarts. NIMS and `sendmail` cannot run on the same server.
- ♦ Check the `/etc/syslog.conf` file for a line that starts with `mail.*`. If it exists, comment it out. In debug mode, mail produces enough syslog messages to fill most disks in a short period of time.

Installing the NIMS Software on Linux

- 1 Log in as `root` > mount the NIMS CD. See your Linux documentation for instructions.

You have several options for installing NIMS. You can install directly from the CD. You can copy the contents of the CD into a temporary directory on your Linux server. You can FTP the contents of the CD or temporary directory to a remote server.

The files and directories you need access to during installation are the `pinstall.lin` script, the `NIMS2.5-1.i386.rpm` file, and the `Pervasive` directory (if you have not already installed Pervasive).

- 2 Change to the directory where the `pinstall.lin` script, the `NIMS-2.5-1.i386.rpm` file, and the `Pervasive` directory are located > enter `./pinstall.lin` at the command prompt.

The `pinstall.lin` script performs the following actions:

- ♦ Verifies that NDS for Linux has been installed
- ♦ Checks to determine if Pervasive has been installed; if not, it installs Pervasive
- ♦ Copies the NIMS files to the installation directory
- ♦ Starts the `nimsext.sh` script

- 3 Type the administrator name > press Tab > type the password > press Enter.

You might need to wait a few moments before continuing. Do not press any keys while waiting. Please be patient.

- 4 When prompted, select Add Schema Extensions > press Enter > select Configure the Server > press Enter > follow the on-screen instructions to continue.

If you choose not to have the installation program configure the server for you, you must create NIMS objects manually. See [Chapter 2, “Planning and Configuring Your NIMS System,” on page 35](#) and [Chapter 3, “Configuring NIMS Objects and Agents,” on page 61](#).

- 5 In the Configuration Parameters dialog box, provide the following information to configure your NIMS server, pressing Tab to move from field to field:

Enter the name of the Messaging Server object in NDS.

Enter the name of the primary domain to be serviced by your NIMS system.

Enter the IP address of one or two DNS servers that will resolve host names into IP addresses for your NIMS system.

- 6** Select the NIMS agents to create NDS objects for, pressing Tab to move from field to field and using the Spacebar to select or deselect:

The SMTP Agent is the means by which messages enter and leave your NIMS system across the Internet.

The POP Agent provides mailbox access for users with any POP3 email client.

The IMAP Agent provides mailbox access for users with any IMAP4 email client.

The WebMail Agent provides mailbox access to users' mailboxes by way of any Web browser.

Forwarding is provided by the AutoReply Agent, which also lets users set up an automated email response when they are not monitoring their mailboxes.

The Alias Agent enables your NIMS system to recognize usernames in a variety of formats.

The Finger Agent lets finger clients find out information about NIMS users.

LDAP support is provided by the Address Book Agent, which allows users to access address book information in NDS.

The AntiSpam Agent protects your NIMS system from UBE (unsolicited bulk email) or SPAM messages.

The Proxy Agent lets users consolidate messages from other POP3 and IMAP4 email accounts into their NIMS mailboxes.

For detailed information on each NIMS agent, see **Chapter 3, "Configuring NIMS Objects and Agents,"** on page 61.

- 7** Continue to follow the installation instructions on the screen until you have exited the NIMS installation program.

Starting NIMS on Linux

On Linux, the NIMS software is installed in `/usr/local/nims` and its subdirectories. The NIMS startup script on Linux is `/etc/rc.d/init.d/nims`. Use the following commands to start and stop your NIMS system:

```
/etc/rc.d/init.d/nims start  
/etc/rc.d/init.d/nims stop
```

Continue with [“Initial NIMS System” on page 22](#)

Initial NIMS System

Your initial NIMS system has the following characteristics:

- ♦ The NIMS Internet Services container object has been created in your NDS tree.
- ♦ Your NIMS system consists of a single messaging server.
- ♦ If you are using NetWare, the message store and message queue have been created by default on the SYS: volume of the messaging server. If you are using Solaris or Linux, the message store and message queue have been created by default in `/usr/nims`.
- ♦ All NIMS agents are associated with that one messaging server.

The following sections explore the components of your NIMS system in detail:

- ♦ [“Internet Services Container” on page 22](#)
- ♦ [“Messaging Server” on page 23](#)
- ♦ [“Message Store” on page 23](#)
- ♦ [“Message Queue” on page 23](#)
- ♦ [“NIMS Agents” on page 23](#)

Internet Services Container

During initial installation, the installation program extended the NDS schema and created the Internet Services container object at the root of your NDS tree.

A single NIMS system cannot span multiple trees. However, NIMS systems can communicate between trees. For more information, see [“NIMS System Must Service Users in Multiple NDS Trees” on page 167](#).

Messaging Server

During initial installation, the installation program created a Messaging Server object in the Internet Services container. The Messaging Server object represents the physical server where you installed the NIMS software. Your NIMS system can consist of a single messaging server or many messaging servers. The differences between these configurations are summarized in [“Standalone Configuration” on page 25](#) and [“Distributed Configuration” on page 26](#).

Message Store

The message store holds users’ mailboxes and messages. All other information required by your NIMS system is stored in NDS. For a complete discussion of the structure and contents of the message store, see [Appendix B, “NIMS Directory Structure and Message Processing,” on page 151](#).

In addition to the main message store on the messaging server, you can create additional message stores for each context where users are located. See [“Creating Local Message Stores for User Contexts” on page 136](#)





Message Queue

Each message store has an associated message queue. The message queue holds messages while they are being processed. Messages pass through the message queue as they are entering or leaving your NIMS system. For a complete discussion of how messages flow through the message queue, see [Appendix B, “NIMS Directory Structure and Message Processing,” on page 151](#).

NIMS Agents

During initial installation, NIMS Agent objects were created in the Messaging Server container. The NIMS agents can be combined in a variety of configurations and still maintain the functionality of a single, integrated messaging system. The table below lists all the NIMS agents and summarizes their contributions to your NIMS system:

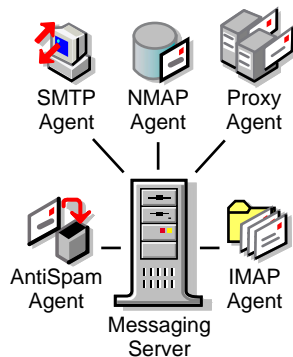
Agent Object	Agent Name	Agent Function
		
		
		
		
		
		
		
		
		
		
		

Agent Object	Agent Name	Agent Function
		
		
		
		

See [Chapter 3, “Configuring NIMS Objects and Agents,”](#) on page 61 for complete information about each agent.

Standalone Configuration

A standalone system configuration is appropriate for your NIMS system if a single, standalone messaging server is sufficient to handle all local message traffic.



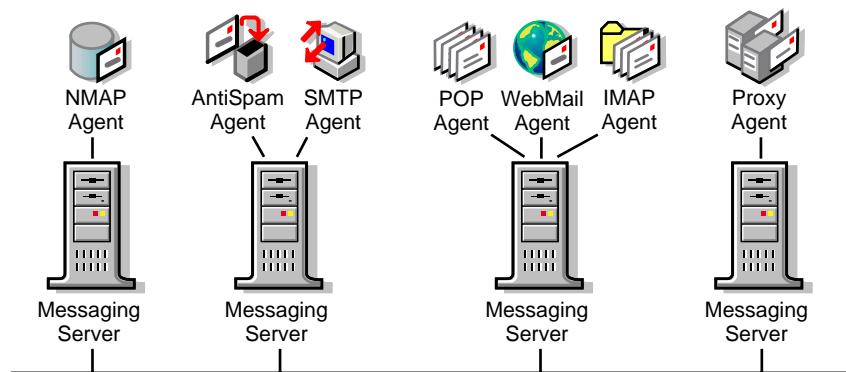
There are two situations where you would set up a single, standalone messaging server:

- ♦ You are setting up a NIMS system where a single messaging server can provide all necessary message processing for all of your users. This type of standalone messaging server is described in detail in [“Single Server Tree” on page 39](#) and [“Single Messaging Server” on page 41](#).
- ♦ Your NIMS system includes users who are located across a slow network link. For best performance throughout your NIMS system, you can set up those users on their own standalone messaging server that is linked to the rest of your NIMS system in a way that does not reduce the performance of the rest of your NIMS system. This type of standalone messaging server is described in detail in [“Hub-and-Spoke Messaging System” on page 52](#).

An advantage to a NIMS system is that if your email needs outgrow a single server, it is easy to add more servers to your NIMS system. You can convert a standalone NIMS system into a distributed NIMS system without replacing existing servers with larger servers and without even interrupting email service to your users.

Distributed Configuration

A distributed system configuration is appropriate for a larger NIMS system where multiple, distributed messaging servers are required to handle the volume of message traffic. A distributed configuration allows you to balance the email load over multiple servers while still managing your NIMS system as a single logical unit.



There are a wide variety of situations where you would set up distributed messaging servers, including:

- ♦ You want to create message stores on several different servers. You could configure each as a messaging server, with at least the NMAP Agent running on each server.
- ♦ You want to provide fast response for email client users. You could configure one or more messaging servers with just the POP, IMAP, and WebMail Agents running so that other NIMS processing wouldn't slow down client responsiveness.
- ♦ You want to provide a list server for your email users and you anticipate substantial list server activity. You could configure one or more messaging servers with just the List Agent running so that other NIMS processing wouldn't slow down list server responsiveness.

All distributed messaging servers must be in the same NDS tree. Usually, all Messaging Server objects are located in the Internet Services container. Distributed messaging servers look for other Messaging Server objects in the Internet Services container. Distributed messaging servers are described in detail in “[Distributed Messaging Servers](#)” on page 48 and “[Hub-and-Spoke Messaging System](#)” on page 52.

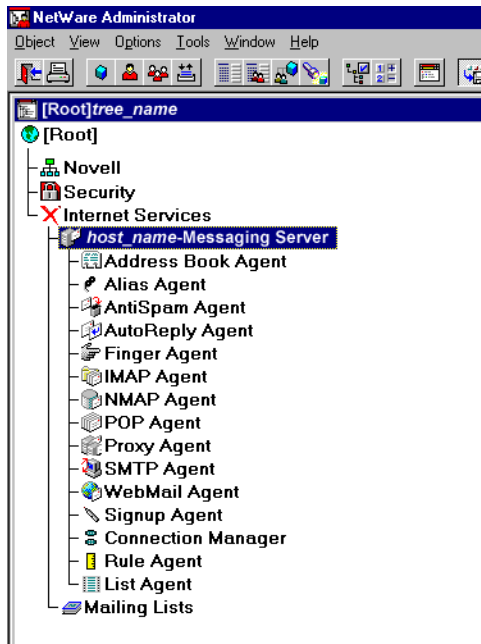
NIMS System Administration

You have several tools for administering your NIMS system:

- ♦ “[Using NetWare Administrator](#)” on page 27
- ♦ “[Using WebAdmin](#)” on page 29
- ♦ “[Using NDS Manager](#)” on page 30

Using NetWare Administrator

NetWare Administrator is a Windows-based administration tool used to manage NDS. During installation, the NIMS snap-in to NetWare Administrator was installed in the PUBLIC\WIN32\SNAPINS directory of your NetWare server, so that you can create and modify NIMS objects.



When you modify any NIMS Agent object, NetWare Administrator automatically reloads the corresponding NLM program on the messaging server. This is convenient when managing NIMS agents on local NetWare servers. However, when managing NIMS agents on remote NetWare servers, NetWare Administrator may reload the agent NLM program before the changes are actually replicated on the messaging server. Consequently, you must manually reload the agent NLM program on the remote NetWare server, for example, by using Telnet or RCONSOLE.

To prevent NetWare Administrator from automatically reloading an agent NLM program when the corresponding Agent object is modified, set the following key in the Windows* Registry to Off:

```
HKEY_CURRENT_USER
    Software
        Novell
            Internet Messaging system
                2.5
                    Auto NLM Reload
```

NetWare Administrator cannot restart NIMS agents running on Solaris or Linux servers, so this issue does not arise. You must always manually restart

a NIMS agent on Solaris or Linux after modifying its properties in NetWare Administrator. See “[Restarting Individual Agents](#)” on page 142.

Changes to User objects do not require restarts to take effect.

Using WebAdmin

If you would prefer to manage NIMS from your Web browser, either locally or remotely, you can use WebAdmin instead of NetWare Administrator. All of the same capabilities are available in both environments.

To use WebAdmin:

- 1 On a NetWare 5.x server, enter **webadmin** at the console prompt.

or

On a NetWare 4.1x server, enter **load webadmin** at the console prompt.

or

On a Solaris server, enter **/opt/NOVLnims/webadmin.sh**.

or

On a Linux server, enter **/usr/local/nims/webadmin.sh**.

By default, WebAdmin uses port 81 for HTTP and port 444 for SSL. For information about WebAdmin startup switches, see “[WEBADMIN Startup Command and Switches](#)” on page 139.

- 2 In your Web browser, enter the URL or host name of the server where you installed NIMS, including port number 81 or 444, to display the WebAdmin page. For example:

`http://127.5.4.1:81`

`http://127.5.4.1:444`

- 3 When prompted, provide the administrator username and password to display the WebAdmin page.

If the user does not exist in the server's container, you must provide the user's context as well. For example, admin.corpsrvr2.abcmail.

- 4** Use the links in the Objects box to navigate through your NDS tree.

Click Help on any page for additional instructions.

Because it is browser-based, WebAdmin is platform independent; you can manage your NIMS messaging system on virtually any operating system for which there is an Internet-standard browser.

WebAdmin does not load or unload agent programs on any platform. When modifying Agent objects in WebAdmin, you must manually reload the corresponding agent programs on the messaging server, for example, by using Telnet or RCONSOLE. See [“Restarting Individual Agents” on page 142](#).

Requiring you to manually reload modified agent programs is an intentional security provision for the browser-based interface. Should someone gain unauthorized access to your system through WebAdmin, they cannot bring down your messaging system.

Using NDS Manager

Configuring your complete NIMS system as described in [Chapter 2, “Planning and Configuring Your NIMS System,” on page 35](#) may require creating and replicating NDS partitions. These activities are not available in

For those not familiar with NDS Manager, the following topics provide a brief overview:

- ♦ “Accessing NDS Manager” on page 31
- ♦ “Creating a Partition” on page 31
- ♦ “Replicating NDS Objects” on page 31

- 2** Browse to and select the remote server where you want to replicate the partition > click OK.

Depending on the size of your system, you may need to wait a while before the partition is locally available on the remote server.

Supported Standards

NIMS supports the major Internet open standards, providing seamless messaging between all email clients that use these standards. This broad-based support eliminates the need for gateways and reduces file translation errors, all without degrading system performance.

An open standard is a non-proprietary, industry-wide standard defined in a public forum known as a Request for Comment (RFC) document. Support for any one of these standards is based on compliance with its associated RFC definition. NIMS fully supports these Internet standards because it complies with the current RFC definition.

NIMS supports the following major open standards:

- ♦ “POP3 and IMAP4” on page 32
- ♦ “SMTP” on page 33
- ♦ “LDAP” on page 33
- ♦ “SSL” on page 33
- ♦ “HTTP” on page 33
- ♦ “MIME and S/MIME” on page 34
- ♦ “NMAP” on page 34

For a complete listing of NIMS supported standards, see [Appendix F, “Supported Standards,”](#) on page 187.

POP3 and IMAP4

Supporting both Post Office Protocol 3 (POP3) and Internet Mail Access Protocol 4 (IMAP4) standards, NIMS is compatible with any client email application including GroupWise[®], Microsoft Outlook[®] Express, Netscape Communicator[®], Eudora[®], Pegasus[®], and other integrated or standalone email clients. See [“POP Agent”](#) on page 85 and [“IMAP Agent”](#) on page 86.

SMTP

NIMS supports Simple Mail Transfer Protocol (SMTP), a protocol used to transfer messages from server to server. Because NIMS supports SMTP, it is compatible with email servers on the Internet and most TCP/IP systems, thereby providing native SMTP/IP routing. See [“SMTP Agent” on page 78](#).

LDAP

Lightweight Directory Access Protocol (LDAP) is an address book protocol. It enables applications to access a directory service, such as NDS eDirectory , Netscape Directory Server*, Microsoft Active Directory*, or one of the many Web-based address books, in order to locate organizations, individuals, or any other resource within that directory.

LDAP compatibility means that NIMS can be integrated with any LDAP-compliant mail client to give the user address book access to information in NDS. NIMS also enables users to access any LDAP compliant address book within its browser-based interface, WebMail.

NIMS supports a read-only subset of LDAP3 enabling it to perform address book queries. See [“Address Book Agent” on page 93](#).

SSL

NIMS protects the integrity of the system by supporting the Secure Sockets Layer (SSL) 3.0 protocol. Using SSL 3.0, NIMS ensures secure email transmissions, remote administration, user self-administration (such as changing passwords) and user authentication over the Internet. NIMS supports SSL on all protocols including POP3, IMAP4, SMTP, and HTTP. See [“Messaging Server: Security” on page 69](#) and [Appendix D, “Setting Up SSL,” on page 171](#).

HTTP

HyperText Transport Protocol (HTTP) support allows users to access their mailboxes from any standard Web browser. See [“Using the NIMS WebMail Client” on page 122](#)

HTTP support also enables Web-based administration. System administrators can manage NIMS’ user and messaging configurations from any standard Web browser. See [“Using WebAdmin” on page 29](#).

MIME and S/MIME

NIMS supports Multipurpose Internet Mail Extensions (MIME) for sending and receiving messages with rich content. NIMS also supports S/MIME (Secure MIME) encrypted messages for secure communications between message senders and receivers.

NMAP

Networked Messaging Application Protocol (NMAP) is an RFC-style protocol used to access user mailboxes and message queues in the NIMS messaging system. See [“NMAP Agent” on page 70](#).

Additional functions such as fax, voice mail, and list servers can be integrated with NIMS through NMAP-compliant applications.

2

Planning and Configuring Your NIMS System

In [Chapter 1, “NIMS System Overview,” on page 11](#), you reviewed your initial NIMS system, which you created by following the installation instructions in the *NIMS Quick Start* or in [“Initial NIMS Installation” on page 11](#).

There are two steps to transforming your initial NIMS system into your complete NIMS system:

- ♦ [“Understanding How NIMS and NDS Work Together” on page 35](#)
- ♦ [“Selecting and Implementing the Configuration for Your Complete NIMS System” on page 38](#)

Understanding How NIMS and NDS Work Together

NIMS uses NDS[®] exclusively to store and look up user and server configuration information. The only things not stored in NDS are the messages. Because of this complete dependence on NDS, you as a NIMS administrator should have at least a basic understanding of NDS. The following topics provide an overview of NDS concepts that are especially important when configuring your NIMS system:

- ♦ [“Why Should I Use a Directory Like NDS?” on page 36](#)
- ♦ [“How Do I Optimize NDS for NIMS?” on page 36](#)
- ♦ [“Which NDS Partitions Contain Information That NIMS Needs?” on page 37](#)

For complete NDS documentation, visit the [Novell Product Documentation site \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

Why Should I Use a Directory Like NDS?

A directory like NDS provides a common database for networked applications to store and look up information about network users and resources.

Applications that do not use a directory must maintain their own copy of information for each user. Directories simplify administration by providing a single source of information for several applications, thus eliminating the need to synchronize additions and modifications to users and applications. For example, an ISP can provide email, FTP, Web, and RADIUS* services that share a common password. When a user changes his or her password, it is automatically changed for all applications.

If your organization already uses NDS, the benefits will be immediately evident. Email accounts do not need to be created. You supply NIMS with a list of NDS contexts, then all users in those contexts automatically have access to NIMS services. Email services are based on the User objects already in existence. In addition, NDS groups, contexts, and organization roles are immediately addressable by NIMS.

In addition, NIMS administration and maintenance tasks are greatly simplified. Because of NIMS' complete integration with NDS, all system, user, and directory configurations can be managed from a single location using NetWare Administrator or WebAdmin. See [“NIMS System Administration” on page 27](#).

How Do I Optimize NDS for NIMS?

NIMS and other Novell directory-enabled applications do not need to know where NDS stores information. Applications merely request that NDS find or store values for specific objects; NDS takes care of the rest. However, how far NDS has to go to find or store information makes a big difference in an application's responsiveness to a user request. NDS-enabled applications perform best when the information is stored on the same server, but will perform adequately when the information is stored on a server on the same high-speed LAN.

NDS can be configured to maintain a copy of the directory on any server in the tree. In NDS terminology, a copy of the directory is called a replica. Local replicas allow NDS-enabled applications to perform better, but also cause NDS to need more network bandwidth to keep all the replicas synchronized. NetWare automatically replicates the root partition on the first three servers in the tree. Subsequent servers do not automatically have local access to NDS data. By default, they must reference NDS over the network. This issue

becomes critical when an organization has users on both sides of a slow WAN link and users at the remote locations want the same high-speed performance as users on the main LAN.

One way to reduce the NDS need for network bandwidth is to replicate only the part of the directory needed by the applications running on that server. NDS allows you to break the directory into pieces called partitions, which allows you to replicate just the partitions that hold information needed by an application.

Which NDS Partitions Contain Information That NIMS Needs?

NIMS servers need quick access to Messaging Server objects and to User objects for which it will provide email services. Access needs differ depending on whether the messaging servers are organized into a standalone or distributed configuration. For a review of these configuration alternatives, see [“Standalone Configuration” on page 25](#) and [“Distributed Configuration” on page 26](#). By default, NIMS servers are configured for use in a distributed configuration.

NDS Requirements for Distributed Messaging Servers

Distributed messaging servers need quick read/write access to the following NDS containers:

- ♦ Internet Services container (see [“Internet Services” on page 63](#))
- ♦ All contexts listed in all NMAP Agent objects (see [“NMAP Agent: Context” on page 75](#))

Because NIMS creates the Internet Services container at the root of the tree, Internet Services belongs to the root partition by default. If you do not want to replicate the root partition to the NIMS messaging servers, you can create a separate partition for the Internet Services container.

NDS Requirements for Standalone Messaging Servers

Standalone messaging servers need quick read/write access to the following NDS containers:

- ♦ The context where the Messaging Server object exists (see [“Messaging Server” on page 64](#))
- ♦ All contexts listed in the local NMAP Agent object (see [“NMAP Agent: Context” on page 75](#))

Standalone messaging servers are often created in the same context as the users they service in order to minimize the number of partitions that need to be created and replicated.

To understand how to meet these NDS requirements, you should consider them in the context of your NIMS system configuration. In general, NIMS messaging systems fall into one of five configurations described in detail in [“Selecting and Implementing the Configuration for Your Complete NIMS System” on page 38](#).

Selecting and Implementing the Configuration for Your Complete NIMS System

The table below summarizes five general system configuration types:

Configuration	Description
---------------	-------------

not

If you are unsure which configuration to implement, use the following questions to help you decide:

Question 1

No

Yes

Question 2:

No

Yes

Question 3:

No

Yes

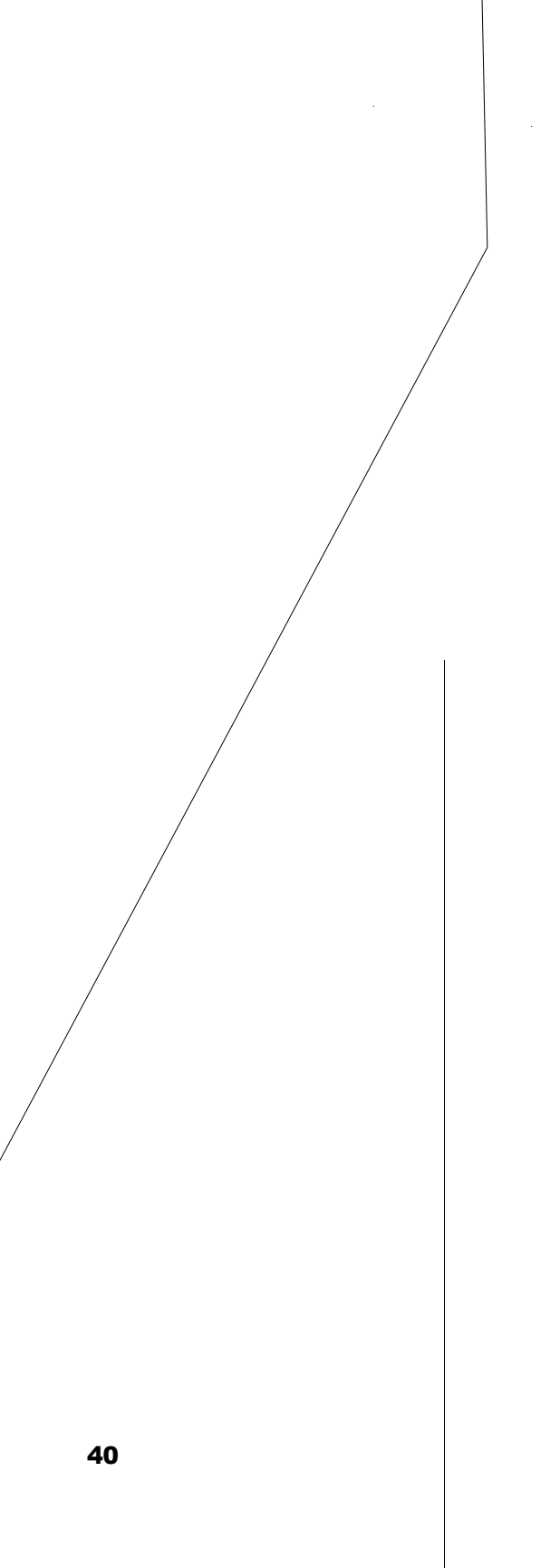
Question 4:

No

Yes

Single Server Tree

For a single server tree, your initial NIMS system, as created by following the instructions in the *NIMS Quick Start* or in “**Initial NIMS Installation**” on page 11, is your complete NIMS system.



message store before you put your NIMS system into production. See “Configuring the NMAP Agent” on page 72 and “NMAP Agent: Parameters” on page 73 for instructions on moving the initial message store to a preferred location.

Continue with “Configuring the NIMS Agents in a Single Server Tree System” on page 41.

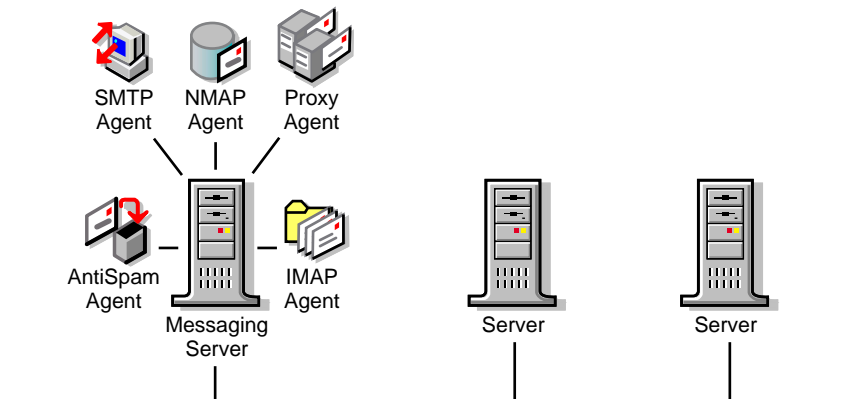
Configuring the NIMS Agents in a Single Server Tree System

Once your NIMS system configuration is complete, continue with Chapter 3, “Configuring NIMS Objects and Agents,” on page 61 to make sure that the NIMS messaging server and agents are configured to meet the needs of your NIMS system.

Single Messaging Server

In a single messaging server system, a dedicated messaging server is integrated into an organization’s existing multiple-server network, where NDS is in use throughout the network. This configuration is common in business and education environments because it is capable of handling a considerable volume of messaging traffic and it allows you to reuse User objects that already exist in NDS.

For a single messaging server system, your initial NIMS system, as created by following the instructions in the *NIMS Quick Start* or in “Initial NIMS Installation” on page 11, can easily become your complete NIMS system.



If the single messaging server configuration is appropriate for your NIMS system, continue with the following tasks:

[illegible]

Choosing the Location of the Message Store in a Single Messaging Server System

In your initial NIMS system as created by following the instructions in the *NIMS Quick Start* or in “Initial NIMS Installation” on page 11, the installation program created the message store in its default location:

- ◆ On a NetWare Server, the default location for the message store is SYS:\NOVONYX\MAIL.
- ◆ On a Solaris or Linux server, the default location is the `/usr/nims` directory.

Depending on the number of users you plan to support, the default location may not be appropriate for your complete NIMS system. It is easy to move the message store before you put your NIMS system into production. See **“Configuring the NMAP Agent” on page 72** and **“NMAP Agent: Parameters” on page 73** for instructions on moving the initial message store to a preferred location.

In addition, if you want to distribute message stores over multiple volumes, you can create local message stores for them. See [“Creating Local Message Stores for User Contexts” on page 136](#).

Continue with “Reconfiguring NDS for a Single Messaging Server” on page 43.

Reconfiguring NDS for a Single Messaging Server

For a review of why NDS reconfiguration is necessary for your NIMS system, see [“Understanding How NIMS and NDS Work Together” on page 35](#).

To fill the NDS requirements for a single messaging server configuration:

- 1** Ensure that a read/write replica of the partition containing the Internet Services container is placed on the NIMS messaging server.

By default, the root partition contains the Internet Services container. If you do not want to replicate the root partition to the messaging servers, you can create a separate partition for the Internet Services container.

A separate Internet Services partition is highly recommended where the NIMS list server will be used extensively. See [“Setting Up a List Server” on page 132](#).

- 2** Ensure that the NIMS messaging server has read/write replicas of all partitions containing user contexts listed in the NMAP Agent object. See [“NMAP Agent: Context” on page 75](#)

Partitioning and replication are typically done with NDS Manager. For assistance using NDS Manager, see [“Using NDS Manager” on page 30](#) and the online help in NDS Manager.

- 3** Continue with [“Configuring the NIMS Agents in a Single Messaging Server System” on page 43](#).

Configuring the NIMS Agents in a Single Messaging Server System

Once your NIMS system configuration is complete, continue with [Chapter 3, “Configuring NIMS Objects and Agents,” on page 61](#) to make sure that the NIMS messaging server and agents are configured to meet the needs of your NIMS system.

Installing the NIMS Software on Each Independent Messaging Server

You should already have installed NIMS on an initial messaging server, which includes extending the NDS schema. Allow time for the schema extensions to synchronize throughout the entire tree before installing the NIMS software on additional servers.

To install the NIMS software on each independent messaging server:

- 1** Follow the installation instructions as provided in the *NIMS Quick Start* or “**Initial NIMS Installation**” on page 11, with the following important exception:
 - ♦ In the list of installation options, select *only* Novell Internet Messaging System Files.
- 2** Continue with “**Configuring Each Independent Messaging Server Manually**” on page 46.

Configuring Each Independent Messaging Server Manually

To manually configure each independent messaging server:

- 1** Follow the instructions in “**Creating a Messaging Server**” on page 64, with the following important exceptions:
 - ♦ Create each Messaging Server object in the same container with the User objects, *not* in the Internet Services container.
 - ♦ In the Official Domain Name field in the Create Messaging Server dialog box, provide the specific domain name to be serviced by each independent messaging server.
- 2** Create the NMAP Agent object for each independent messaging server as described in “**Creating an NMAP Agent Object**” on page 71.
- 3** Continue with “**Turning Off Distributed Processing for Each Independent Messaging Server**” on page 47.

Turning Off Distributed Processing for Each Independent Messaging Server

By default, each messaging server will search the tree for the Internet Services container and its associated Messaging Server objects. Because an independent messaging server is unrelated to other messaging servers in the NIMS system, you should prevent it from searching for other Messaging Server objects.

To configure each independent messaging server:

- 1** Follow the instructions in [“Configuring the Messaging Server” on page 65](#), with the very important exception:
 - ♦ On the Messaging Server object Identification page, select Distributed Processing Disabled. For more information, see [“Messaging Server: Identification” on page 67](#)
- 2** Continue with [“Reconfiguring NDS for Independent Messaging Servers” on page 47](#).

Reconfiguring NDS for Independent Messaging Servers

For a review of why NDS reconfiguration is necessary for your NIMS system, see [“Understanding How NIMS and NDS Work Together” on page 35](#).

To fill the NDS requirements for an independent messaging server configuration:

- 1** Ensure that a read/write replica of the partition containing the Messaging Server object is placed on the NIMS messaging server.
- 2** Ensure that the NIMS messaging server has read/write replicas of all partitions containing user contexts listed in its own NMAP Agent object. See [“NMAP Agent: Context” on page 75](#)

By creating the Messaging Server in one of the user contexts, one replica can usually cover both requirements.

Partitioning and replication are typically done with NDS Manager. For assistance using NDS Manager, see [“Using NDS Manager” on page 30](#) and the online help in NDS Manager.

- 3** Continue with [“Configuring the NIMS Agents for Each Independent Messaging Server” on page 48](#).

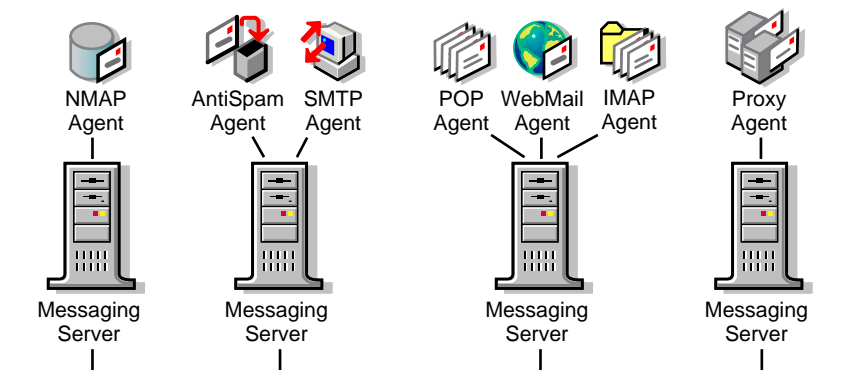
Configuring the NIMS Agents for Each Independent Messaging Server

Once your NIMS system configuration is complete, continue with [Chapter 3, “Configuring NIMS Objects and Agents,”](#) on page 61 to make sure that the NIMS messaging servers and agents are configured to meet the needs of each independent messaging server.

Distributed Messaging Servers

In a distributed messaging server system, the NIMS agents are distributed across multiple servers in order to distribute the message processing load. Distributed messaging server systems are most often used in ISP, ASP, and multi-LAN organizations. These organizations require multiple messaging servers due to the volume of messaging traffic, performance requirements, or the local distribution of the network.

In such environments, two or more messaging servers can be configured to work together as a single, integrated system. In this way, messaging system functions can be distributed across multiple servers to provide load balancing, fault tolerance, and speed. For a review of agent distribution strategies, see [“Distributed Configuration”](#) on page 26.



For a practical example of this configuration, see [“Distributed Messaging Server System Example”](#) on page 182.

If the distributed messaging server configuration is appropriate for your NIMS system, continue with the following tasks:

Task	Purpose
------	---------

Choosing the Location of the Message Store in a Distributed Messaging Server System

In your initial NIMS system as created by following the instructions in the *NIMS Quick Start* or in “[Initial NIMS Installation](#)” on page 11, the installation program created the message store in its default location:

- ♦ On a NetWare Server, the default location for the message store is SYS:\NOVONYX\MAIL.
- ♦ On a Solaris or Linux server, the default location is the `/usr/nims` directory.

Depending on the number of users you plan to support, the default location may not be appropriate for your complete NIMS system. It is easy to move the message store before you put your NIMS system into production. See “[Configuring the NMAP Agent](#)” on page 72 and “[NMAP Agent: Parameters](#)” on page 73 for instructions on moving the initial message store to a preferred location.

When you set up additional distributed messaging servers after your initial NIMS installation, you can select the desired message store location as you manually create each NMAP Agent object.

Continue with “[Installing Additional NIMS Software on Each Distributed Messaging Server](#)” on page 50

Installing Additional NIMS Software on Each Distributed Messaging Server

You should already have installed NIMS on an initial messaging server, which includes extending the NDS schema. Allow time for the schema extensions to synchronize throughout the entire tree before installing the NIMS software on additional servers.

To install the NIMS software on each distributed messaging server:

- 1** Follow the installation instructions as provided in the *NIMS Quick Start* or “[Initial NIMS Installation](#)” on page 11, with the following important exceptions:
 - ♦ In the list of installation options, select *only* Novell Internet Messaging System Files.
 - ♦ In the list of NIMS agents, deselect the NIMS agents for which you do not want to create objects on this distributed messaging server.
- 2** Continue with “[Configuring Each Distributed Messaging Server Manually](#)” on page 50.

Configuring Each Distributed Messaging Server Manually

To manually configure each distributed messaging server:

- 1** Follow the instructions in “[Creating a Messaging Server](#)” on page 64.
- 2** Create the NMAP Agent object for the distributed messaging server as described in “[Creating an NMAP Agent Object](#)” on page 71.
- 3** Continue with “[Configuring Trusted Hosts for Distributed Messaging Servers \(Optional\)](#)” on page 51.

Configuring Trusted Hosts for Distributed Messaging Servers (Optional)

When NIMS agents need access to the message store or message queue, they create an IP connection to the associated NMAP Agent and request the information they need. By default, the NMAP Agent requires NIMS agents that run on other servers to authenticate before it carries out their requests. For faster processing, you can configure the NMAP Agent to skip the authentication process for specified IP addresses, which become "trusted hosts" to the NMAP Agent.

- ♦ For Solaris or Linux servers, trusted host status should not be granted unless login access to the trusted host servers is restricted to the system administrator.
- ♦ For NetWare servers, trusted host status can improve performance

If your NIMS system would *not* benefit from trusted hosts, skip to [“Reconfiguring NDS for Distributed Messaging Servers” on page 51](#).

To configure trusted hosts using NetWare Administrator:

- 1** Follow the instructions in [“Configuring the NMAP Agent” on page 72](#) and [“NMAP Agent: Trusted Hosts” on page 77](#)
- 2** Continue with [“Reconfiguring NDS for Distributed Messaging Servers” on page 51](#).

Reconfiguring NDS for Distributed Messaging Servers

For a review of why NDS reconfiguration is necessary for your NIMS system, see [“Understanding How NIMS and NDS Work Together” on page 35](#).

To fill the NDS requirements for a distributed messaging system configuration:

- 1** Ensure that a read/write replica of the partition containing the Internet Services container is placed on at least one of the NIMS messaging servers.

By default, the root partition contains the Internet Services container. If you do not want to replicate the root partition to the messaging servers, you can create a separate partition for the Internet Services container.

- 2 Ensure that at least one of the NIMS messaging servers has read/write replicas of all partitions containing the user contexts listed in all NMAP Agent objects in the system. See [“NMAP Agent: Context” on page 75](#).

NIMS runs more efficiently when the messaging servers that have replicas have a complete set of all replicas needed for NIMS. This allows NDS to use the same server for all lookups instead of switching back and forth to find different User and Server objects.

Partitioning and replication are typically done with NDS Manager. For assistance using NDS Manager, see [“Using NDS Manager” on page 30](#) and the online help in NDS Manager.

- 3 Continue with [“Configuring the NIMS Agents in a Distributed Messaging Server System” on page 52](#).

Configuring the NIMS Agents in a Distributed Messaging Server System

Once your NIMS system configuration is complete, continue with [Chapter 3, “Configuring NIMS Objects and Agents,” on page 61](#) to make sure that NIMS messaging servers and agents are created and configured to meet the needs of each distributed messaging server.

Hub-and-Spoke Messaging System

A hub-and-spoke messaging system typifies government and enterprise messaging systems. In these environments, the messaging system is geographically dispersed. The physical distance between messaging servers introduces a new set of configuration requirements. To support this system, messaging servers must be able to work together without generating unnecessary network traffic across the slow WAN links.

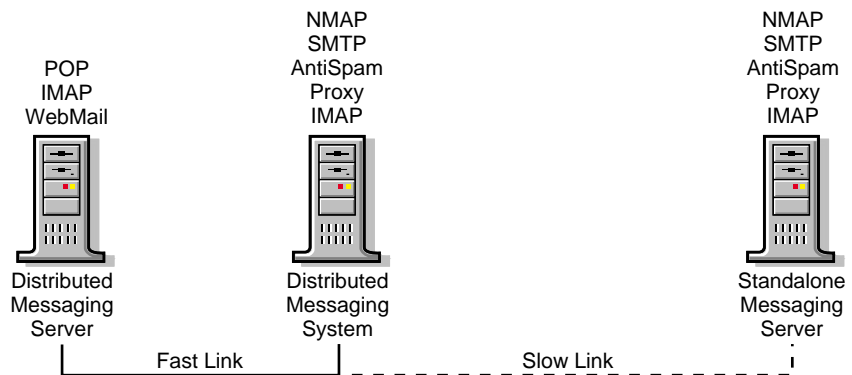
In designing a hub-and-spoke messaging system, you should first consider what kinds of links you have between locations. Locations that connect to the hub over fast links can employ the same strategies used in a regular distributed messaging server system. See [“Distributed Messaging Servers” on page 48](#). However, locations that connect to the hub over slow links cannot use those same strategies.

Due to limited bandwidth and speed, the primary concern in a hub-and-spoke environment is to minimize network traffic across slow WAN links. Another concern is preventing messaging servers in remote locations from searching

the NDS tree for the Internet Services container and User objects that have not been replicated to the remote location. Searching the tree over a slow WAN link not only increases network traffic, but it compromises the functionality of the system because the NDS query will time out before it is able to locate the needed information. If the query times out, the sender receives a message indicating that the user does not exist.

One way of addressing these concerns is to locate messaging servers only in the hub location. Users in remote locations would then have to access messaging servers at the hub. While this option reduces network traffic and avoids the issue of having servers in remote locations search the entire tree, it does not provide optimal performance for the remote users. Users in remote locations would experience perceivably slow service as they wait to send and download mail over the WAN.

You can provide fast and reliable messaging services to users in remote locations by installing a standalone messaging server in each remote location. A standalone messaging server looks for User objects only in local contexts. Network traffic is reduced because all messaging operations take place on the local standalone server. Because the standalone messaging server is in the users' local environment, users experience perceivably faster service when using their email clients (though for messages that traverse the WAN, actual message delivery time does not change).



For a practical example of this configuration, see [“Hub-and-Spoke Messaging System Example” on page 183](#).

If the hub-and-spoke messaging system configuration is appropriate for your NIMS system, continue with the following tasks:

Task	Purpose
------	---------

Installing the NIMS Software on Each Remote Server

After installing the NIMS software on distributed messaging servers at your central location, you should then install the NIMS software on remote servers located across the WAN. If the administrators of the remote servers do not have access to NIMS CDs, you should provide the NIMS software to them in some other way.

- ♦ If the remote server is a NetWare server, you can mount the CD remotely so that, when using NWCONFIG, the administrator of the remote server can specify the software location using the following format:

server_name\volume:NIMS2_5

- ♦ If the remote server is a Solaris or Linux server, you can FTP the contents of the NIMS CD to the remote server so the administrator there can perform the installation.

You should already have installed NIMS on an initial messaging server, which included extending the NDS schema. Allow time for the schema extensions to synchronize throughout the entire tree before installing the NIMS software on remote servers.

Once the software is available on each remote server, the administrator at the remote location can:

- 1 Follow the installation instructions as provided in the *NIMS Quick Start* or “**Initial NIMS Installation**” on page 11, with the following important exception:
 - ♦ In the list of installation options, select *only* Novell Internet Messaging System Files.
- 2 Continue with “**Configuring Each Remote Messaging Server Manually**” on page 55.

Configuring Each Remote Messaging Server Manually

To manually configure each remote messaging server:

- 1 Follow the instructions in “**Creating a Messaging Server**” on page 64, with the following important exception:
 - ♦ Create the Messaging Server object in the same container with the User objects on the remote messaging server, *not* in the Internet Services container.

- 2 Create the NMAP Agent object for the independent messaging server as described in [“Creating an NMAP Agent Object” on page 71](#).
- 3 Continue with [“Turning Off Distributed Processing for Each Remote Messaging Server” on page 56](#).

Turning Off Distributed Processing for Each Remote Messaging Server

By default, each messaging server will search the NDS tree for the Internet Services container and its associated Messaging Server objects. Because a remote messaging server is located across a slow WAN link from the Internet Services container and the other messaging servers in your NIMS system, you should prevent it from searching for NDS objects across the slow link.

To configure a remote messaging server as a standalone messaging server:

- 1 Follow the instructions in [“Configuring the Messaging Server” on page 65](#), with the following important exception:
 - ♦ On the Messaging Server object Identification page, select Distributed Processing Disabled. For more information, see [“Messaging Server: Identification” on page 67](#),
- 2 Continue with [“Forwarding Local Undeliverable Messages to the Central Messaging System” on page 56](#).

Forwarding Local Undeliverable Messages to the Central Messaging System

Once a messaging server’s distributed functionality is turned off, it is essentially isolated from the rest of the messaging system. Users can send and receive messages from users in their local environment, or they can send and receive remote messages. However, they cannot send or receive messages from other messaging servers within their messaging system domain.

To enable users in remote locations to send messages to other users, the remote messaging server must be configured to forward local undeliverable messages. Local undeliverable messages are messages that are addressed to the messaging system domain but where the user portion of the address cannot be found in the current NMAP Agent’s assigned contexts. When the NMAP Agent receives one of these messages, it recognizes that the message belongs to its messaging system domain, but it cannot find the recipient in its assigned context. The message, therefore, is undeliverable.

Configuring the NMAP Agent to forward local undeliverable messages enables the remote messaging server to forward messages that belong to the messaging system domain but are not locally deliverable. Messages are forwarded via the SMTP Agent to another messaging server, which can then route the message for delivery.

To configure the remote NMAP Agent to forward local undeliverable messages to the central messaging system using NetWare Administrator:

- 1** Follow the instructions in [“Configuring the NMAP Agent” on page 72](#), paying special attention to the following setting:
 - ♦ On the Options page, in the Forward Local Undeliverable Messages field, specify the host name or IP address of the server in the central messaging system that is designated to receive messages that are locally undeliverable on the remote messaging server. If you specify an IP address rather than a host name, you must enclose the IP address in square brackets [] to form a valid email address. For more information, see [“NMAP Agent: Options” on page 74](#).
- 2** Continue with [“Creating an Alias for Each Remote Messaging Server” on page 57](#).

Creating an Alias for Each Remote Messaging Server

With the Forward Local Undeliverable Messages option configured for the remote NMAP Agent, the remote messaging server can send messages to the central messaging system. However, there remains the problem of enabling each remote messaging server to receive messages from the central messaging system.

With the current configuration, the distributed messaging servers in the Internet Services container still cannot send messages to remote messaging servers. This is because distributed messaging servers only look in the Internet Services container for other Messaging Server objects. If a Messaging Server object does not exist in the Internet Services container, the distributed messaging servers cannot find it.

For users located in the central messaging system to send messages to users on remote messaging servers, each remote messaging server should have a corresponding Alias object in the Internet Services container.

To create an Alias object using NetWare Administrator:

- 1** Browse to and right-click the Internet Services container > click Create.

- 2** Double-click Alias.
- 3** Provide a unique name for the Alias object.
- 4** Browse to and double-click the remote Messaging Server object.
- 5** Click Create to create the Alias object so that the remote messaging server is represented in the Internet Services container of the central messaging system.

The central messaging system and the remote messaging server are now linked and fully functional. To summarize:

- ♦ Remote users across the slow link can send messages to users in the central messaging system because the NMAP Agent on each remote messaging server has been configured to send local undeliverable messages to a messaging server in the central messaging system.
 - ♦ Remote users across the slow link can receive messages from users in the central messaging system because an Alias object representing each remote messaging server has been created in the Internet Services container so that NMAP Agents in the central messaging system can locate the remote messaging server.
- 6** Continue with “**Configuring Trusted Hosts for Remote Messaging Servers (Optional)**” on page 58.

Configuring Trusted Hosts for Remote Messaging Servers (Optional)

When NIMS agents need access to the message store or message queue, they create an IP connection to the associated NMAP Agent and request the information they need. By default, the NMAP Agent requires NIMS agents that run on other servers to authenticate before it carries out their requests. For faster processing, you can configure the NMAP Agent to skip the authentication process for specified IP addresses, which become "trusted hosts" to the NMAP Agent.

- ♦ For Solaris or Linux servers, trusted ho5.7(eservnee7(t.))TJ.4(s1)-1(h Wu.9(l)6d no

- 1 Follow the instructions in “Configuring the NMAP Agent” on page 72 and “NMAP Agent: Trusted Hosts” on page 77
- 2 Continue with “Reconfiguring NDS for Distributed Messaging Servers” on page 51.

Reconfiguring NDS for Remote Messaging Servers

For a review of why NDS reconfiguration is necessary for your NIMS system, see “Understanding How NIMS and NDS Work Together” on page 35

To fill the NDS requirements for a hub-and-spoke configuration:

- 1 Ensure that a read/write replica of the partition containing the Messaging Server object is placed on the standalone messaging server.
- 2 Ensure that the NIMS messaging server has read/write replicas of all partitions containing user contexts listed in its own NMAP Agent object. See “NMAP Agent: Context” on page 75.

By creating the Messaging Server object in one of the user contexts, one replica can usually cover both requirements.

Partitioning and replication are typically done with NDS Manager. For assistance using NDS Manager, see “Using NDS Manager” on page 30 and the online help in NDS Manager.

- 3 Continue with “Configuring the NIMS Agents for a Remote Messaging Server” on page 59.

Configuring the NIMS Agents for a Remote Messaging Server

One drawback of a remote messaging server is that it cannot share messaging functions with distributed servers in the central messaging system; consequently, the NMAP, SMTP, POP, IMAP, WebMail, AutoReply, Rule, Proxy, Alias, AntiSpam, List, and Finger Agents, along with the Connection Manager, all run locally on a remote messaging server.

An Address Book Agent running on a remote messaging server only returns local users in Address Book searches. However, email clients can be configured to access a distributed Address Book Agent in the central messaging system. For example, see “WebMail Agent: Address Book” on page 92.






Now that your NIMS system configuration is complete, continue with **Chapter 3**, “Configuring NIMS Objects and Agents,” on page 61 to make sure the NIMS messaging servers and agents are created and configured to meet the needs of each remote messaging server.

3

Configuring NIMS Objects and Agents

NIMS has a highly modular architecture. Its product functions are divided among multiple agents. These agents have plug-and-play versatility; they can be combined in a variety of configurations and still maintain the functionality of a single, integrated messaging system. This building block architecture enables NIMS to be easily distributed across multiple servers.

The table below summarizes the functions of the various NIMS objects and agents and links you to the details for their creation and configuration.

Agent Object	Agent Name	Agent Function
		
		
		
		
		

Agent Object	Agent Name	Agent Function
		
		
		
		
		
		
		
		
		
		
		
		

Internet Services

The Internet Services container represents a collection of distributed messaging servers in NDS. It is automatically created during installation at the root of the tree. There can be only one Internet Services container per tree.

The only configurable aspect of the Internet Services container is the Syslog, which provides logging and reporting capabilities that you can use to diagnose problems and fine-tune server performance.

- ♦ On Solaris* and Linux*, the Syslog is part of the operating system. It is typically configured by editing the `/etc/syslog.conf` file. Continue with “[Messaging Server](#)” on page 64
- ♦ On NetWare, the same capabilities are available by configuring the Internet Services container. Continue with “[Configuring the Internet Services Container](#)” on page 63.

Configuring the Internet Services Container

To configure the Internet Services container in NetWare® Administrator:

- 1** Double-click the [Root] object > right-click the Internet Services object > click Details.

The Information page explains the Internet Services object.

- 2** Click Syslog.

The Syslog page is available for the Internet Services object and for NetWare Server objects. The Syslog settings provided for the Internet Services object establish defaults for your NIMS system. Settings provided for individual NetWare Server objects allow you to customize logging for specific servers.

- 3** Select the types of events you want recorded in the Syslog.

Selecting Emergency logs the least information; selecting Debug logs the most information. Settings are cumulative, so if you select Debug, all lesser levels of events are also logged.

- 4** Select Log to File if you want Syslog information saved to disk.

If you do not specify a filename, the Syslog is written to `SYS:\ETC\SYSLOG`. If you specify a filename, the file is written to the `SYS:\ETC\SYSLOG.D` directory. You can specify a full path name to place the Syslog file in a different directory.

5 Click OK to save the default Syslog configuration for your NIMS system.

For additional control of the Syslog on a NetWare server, see “**SYSLOG Commands**” on page 145. For additional statistics-gathering capabilities on a NetWare server, see “**MAIL Commands**” on page 145.

6 Continue with “**Messaging Server**” on page 64.

You can also perform this procedure using WebAdmin. For more information, see “**Using WebAdmin**” on page 29.

Messaging Server

If this is an initial installation and you have followed the installation instructions in the *NIMS Quick Start* or in “**Initial NIMS Installation**” on page 11, the installation program created a Messaging Server object in the Internet Services container. You should configure this Messaging Server object to meet the needs of your NIMS system. Continue with “**Configuring the Messaging Server**” on page 65

If you do not have the installation program configure your messaging server, you can manually create a Messaging Server object for each server where you want to run NIMS agents. Continue with “**Creating a Messaging Server**” on page 64.

Creating a Messaging Server

When you manually create a Messaging Server object, you can create it in either of two locations:

- ♦ Typically, you create the Messaging Server object in the Internet Services container, because distributed messaging servers automatically look for other messaging servers in the Internet Services container.
- ♦ You may want to create the Messaging Server object outside the Internet Services container so that messaging server administration can be distributed across multiple servers or so that the Messaging Server object can be created in the same context as User objects.

By default, Messaging Server objects created outside the Internet Services container will not be recognized by other distributed messaging servers. To integrate these servers with the rest of the messaging system,

Alias objects should be created for them within the Internet Services container. Alias objects enable distributed messaging servers to locate and interact with messaging servers outside the Internet Services container. See [“Hub-and-Spoke Messaging System” on page 52](#) for assistance in setting up this more advanced configuration.

To create a Messaging Server object using NetWare Administrator:

- 1** Browse to and right-click the Internet Messaging object.

or

Right-click another container object where you want to create a Messaging Server object.

- 2** Click Create > double-click Messaging Server.

- 3** Fill in the required fields:

Type a unique name for the Messaging Server object in NDS.

Browse to and select the server that you want to be a NIMS messaging server.

Browse to and select the user assigned to manage the messaging server. The Postmaster receives email notifications about problems with the messaging server and requires more rights than the typical user to correct these problems.

Type the name of the primary domain serviced by your NIMS system.

- 4** Click Create to create the Messaging Server object.

- 5** Continue with [“Configuring the Messaging Server” on page 65](#)

Configuring the Messaging Server

To configure your initial messaging server in NetWare Administrator:

- 1** Browse to and double-click the Internet Messaging object > right-click the Messaging Server object > click Details.
- 2** Click a Details page > configure the Messaging Server object for your NIMS system needs.

-
- 3** When you have finished configuring the messaging server, click OK to save the messaging server configuration.
 - 4** Restart the messaging server. See [“Startup Commands” on page 137](#).
 - 5** Continue with [“Understanding How NIMS and NDS Work Together” on page 35](#).

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Messaging Server: Identification

Displays the full context name of the server that is serving as a NIMS messaging server.

Browse to and select the user assigned to manage the messaging server. The Postmaster receives email notifications about problems with the messaging server and requires more rights than the typical user to correct these problems.

Displays the Internet domain serviced by the messaging server (such as companyname.com or isp.net). If the NMAP Agent will run on this messaging server, the official domain name will be the default domain for users within the NMAP Agent's context. In addition, all system messages, such as those sent to the Postmaster, will use this domain.

The official domain name must be registered in DNS before the messaging system can send and receive mail via the Internet.

NIMS can share an Internet domain with other messaging systems. NIMS will run alongside any application that supports Internet standards including groupware applications such as Novell GroupWise®, Lotus Notes*, and Microsoft* Exchange. For information about domain sharing, see [“Forward Local Undeliverable Messages” on page 75](#).

You can associate the Messaging Server object with a different domain name by changing the official domain in this field.

Specify the volume and, optionally, the directory where the NIMS agents write temporary files.

Specify the volume and, optionally, the directory where the NIMS alias database, address book, and queue client files are stored.

Specify the IP address of one or more DNS servers that resolve host names into IP addresses.

The Connection Manager provides user authentication services by tracking the IP addresses of client users. The POP, IMAP, and SMTP Agents can all make use of the Connection Manager. If you have configured a Connection Manager for your NIMS system, select Connection Manager > browse to and select a Connection Manager object.

For more information about the Connection Manager, see [“Connection Manager” on page 110](#).

If your NIMS system has only one messaging server, select Distributed Processing Disabled, because distributed processing is not needed.

If your NIMS system has multiple messaging servers, the messaging servers attempt to provide email services to all users in the system. If your NIMS system includes messaging servers isolated from the rest of the NIMS system by a slow network link, performance is improved by limiting such message servers. When you are configuring a messaging server that is located across a slow link from your main system, you can select Distributed Processing Disabled, which causes that messaging server to operate in standalone mode, without attempting to communicate with other messaging servers. For more information, see [“Hub-and-Spoke Messaging System” on page 52](#).

Messaging Server: Statistics (NetWare Only)

The Statistics page provides up-to-date resource and performance statistics for a NetWare server, essentially the same statistical information as provided by the MAILCON utility. This can be useful for administrators who do not have access to the server console. By default, the Statistics page includes the following information:

- ♦ The number of local and remote messages that have been queued, received and delivered
- ♦ The total number of recipients of inbound and outbound messages
- ♦ The total number of client connections, that is, the number of people logged in at that moment through the POP, IMAP, or WebMail Agents
- ♦ The total number of server connections, that is, the number of SMTP, WebMail and Proxy connections (users and servers) that are sending messages to the messaging server for processing in the message queue
- ♦ The volume of inbound and outbound mail processed by the messaging server
- ♦ Server uptime

If the server is down, the statistics fields display "n/a."

For comprehensive statistical reports on a NetWare server, launch the MAILCON server utility. For more information, see [“MAILCON \(NetWare Only\)” on page 148](#).

Messaging Server: Security

NIMS supports SSL (Secure Socket Layer) security. SSL protects the information passed between email clients and the messaging server. See [Appendix D, “Setting Up SSL,” on page 171](#) for instructions before configuring the messaging server to use SSL.

SSL does not secure messages leaving your email system. To secure message content, users can use an X.509 client certificate. For more information about X.509 client certificates, consult your client vendor.

Select Allow SSLv2 to configure the messaging server to accept SSLv2 connections if a trusted certificate has been installed. If this option is deselected, SSLv2 connections cannot be used. This is a backward-compatibility option. Most applications have standardized on SSLv3, but you can enable SSLv2 connections to accommodate older clients.

Select Allow SSLv3 to configure the messaging server to accept SSLv3 connections if a trusted certificate has been installed. By using SSLv3, you enable secure data transport between clients and your messaging server. Most systems that are using SSL have standardized on SSLv3.

Select Allow X.509 Client Certification to enable the messaging server to recognize a user's client certificate.

X.509 certificates secure message content by encrypting the message data. X.509 certificates can be also used to authenticate user identity through the use of digital signatures. X.509 certificates are installed at the user's workstation and are managed through the user's mail client.

Although X.509 client certificates are not installed or managed at the server level, when a user with a client certificate connects with the messaging server, the messaging server recognizes the user's identity through his or her client certificate and automatically opens the user's account. Therefore, the user never needs to log in because the system trusts the client certificate.

Be aware that client certificates are actually workstation-specific, not user-specific. Consequently, if you select Allow X.509 Client Certificates, anyone with access to the workstation will have access to the user's email account. If multiple users are using the same workstation or if a user's workstation is not secure, do not select Allow X.509 Client Certificates.

Automatic authentication through client certificates works with IMAP and WebMail clients, but not with POP clients. The POP protocol cannot give the messaging server the client certificate information. Therefore, users with POP email clients must enter their user names and passwords to the NIMS system even though they have a client certificate.

Messaging Server: SNMP Configuration

NIMS supports SNMP (Simple Network Management Protocol) so management tools such as HP OpenView* or Novell® ManageWise® can be used to detect problems, optimize server performance, and obtain long-term trending information.

Provide organization, location, contact, and name information for the messaging server to pass to SNMP applications that request information about the messaging server.

Messaging Server: Status

Displays the IP address of the messaging server and its current status. A messaging server can have a status of Running or Shut Down.

By default, the messaging server is enabled. Select Disable Server > click OK to disable the messaging server.

NetWare Administrator stops the NLM messaging server immediately. As long as its status is Disabled, the messaging server will not restart if you restart the rest of your NIMS system.

NetWare Administrator does not stop the messaging server on Solaris and Linux. You should stop it manually. See [“Restarting Individual Agents” on page 142](#).

NMAP Agent

The NMAP Agent has three very important functions:

- ♦ Managing the message store (where user mailboxes are located)
- ♦ Managing the message queue (where incoming and outgoing messages are processed)
- ♦ Providing IP access to the message store and message queues for all other NIMS agents on port 689

NMAP stands for Network Messaging Application Protocol. It is the messaging protocol used by all NIMS agents to communicate with the NMAP Agent. At least one NMAP Agent must exist in a distributed messaging system. Every standalone messaging server must run an NMAP Agent.

For an illustration of how the NMAP Agent processes messages in the message queue, see [“Message Processing in the Message Queue” on page 154](#).

Any NMAP-compliant application can access the message store and message queues via the NMAP Agent. This enables outside products to be integrated with NIMS to provide additional functions such as fax, voice mail, or list servers.

One NMAP Agent is created when you install the NIMS software on a server. If you want to configure your existing NMAP Agent, skip to [“Configuring the NMAP Agent” on page 72](#). If you want to create an NMAP Agent for a new messaging server, continue with [“Creating an NMAP Agent Object” on page 71](#).

Creating an NMAP Agent Object

To create an NMAP Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add an NMAP Agent > click Create.
- 2** Double-click NMAP Agent.
- 3** Fill in the required fields:

Specify the volume and, optionally, the directory where the NMAP Agent will create the message store and message queue. Because the NMAP Agent needs direct access to the message store, the message store directory should be on the same server where you have installed the NIMS software.

Because NetWare requires free space on the SYS: volume, you should weigh the potential disk space requirements of your messaging system before creating the mail directories on the SYS: volume of a NetWare server.

Browse to and select the NDS context that will be serviced by the current NMAP Agent. When creating the NMAP Agent object, you can select only one user context. However, when configuring the NMAP Agent, you can add multiple user contexts. For additional details, see [“NMAP Agent: Context” on page 75](#)

- 4** Click Create to create the NMAP Agent object.
- 5** If you created the new NMAP Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

6 Continue with “Configuring the NMAP Agent” on page 72

You can also perform this procedure using WebAdmin. For more information, see “Using WebAdmin” on page 29.

Configuring the NMAP Agent

To configure the NMAP Agent using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object > right-click the NMAP Agent to configure > click Details.
- 2** Click a Details page > configure the NMAP Agent for your NIMS system needs.

Details Page	Options
--------------	---------

- 3** After configuring the NMAP Agent, click OK to save the changes.
- 4** If you added or removed contexts, you must restart all messaging servers in a distributed NIMS system, including all remote messaging servers. See [“Startup Commands” on page 137](#).

or

If you changed other NMAP Agent configuration options, you can restart just the NMAP Agent. See [“Restarting Individual Agents” on page 142](#).

- 5** Return to [“Configuring NIMS Objects and Agents” on page 61](#) to select a different NIMS agent to configure.

or

When you have configured all your NIMS agents, continue with [Chapter 4, “Optimizing Your NIMS Messaging Servers,” on page 115](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

NMAP Agent: Parameters

Storage Paths

Allows you to specify the location of the message store and message queues.

Specify the volume and, optionally, the directory where you want the message store to reside. For information about the directory structure of the message store, see [“Message Store Directory” on page 151](#).

Because NetWare requires free space on the SYS: volume, you should weigh the potential disk space requirements of your messaging system before creating the mail directories on the SYS: volume of a NetWare server.

If you need to move the message store, stop the NMAP Agent > move the existing message store directory to its new location > change the location specified in the Message Store field > restart the NMAP Agent. See [“Restarting Individual Agents” on page 142](#).

In addition to the main message store on the messaging server, you can create additional message stores for each context where users are located. See [“Creating Local Message Stores for User Contexts” on page 136](#).

Specify the volume and, optionally, the directory where you want the message queue to reside.

Specify the minimum amount of free space you want to maintain on the volume hosting the message queue. The default is 2048 KB. If the minimum disk space amount is reached, your NIMS system will stop accepting messages, stop logging, and stop message delivery. The system also sends an SNMP trap.

If your mail directories are on the SYS: volume, this option can be used to maintain the free space required by NetWare.

Specify the volume and, optionally, the directory where you want the Single Copy Message Store (SCMS) directory to reside. See [“NMAP Agent: Single Copy Message Store” on page 77](#).

Queue Parameters

Specify the number of minutes the NMAP Agent waits before reprocessing messages that have been left in the queue for any reason. The default is 30 minutes.

Specify how many days the NMAP Agent should wait before removing undeliverable messages from the queue. The NMAP Agent attempts to bounce these messages before removing them. The default is 5 days.

NMAP Agent: Options

Bounced Message Control

It is a common practice for spammers to falsify the From: field so that resulting bounced messages go to a mail server other than their own. This can cause the server that owns the domain specified by the spammers in the From: field to be inundated with thousands of bounced messages in a short period of time. To keep your NIMS system from wasting system resources during such attacks, you can limit the number of bounced messages NIMS will process during a specified time interval.

Select CC Postmaster if you want the Postmaster to receive copies of bounced messages.

Select Limit Bounces To to turn on bounced message control.

- ♦ Specify the time frame, in seconds, during which bounces are counted.
- ♦ Specify the number of bounced messages representing the threshold. If the number of bounced messages exceeds the defined

threshold within the defined time frame, messages are deleted by the NMAP Agent instead of being bounced. This preserves system resources from being lost in handling failed messages.

Forward Local Undeliverable Messages

When the NMAP Agent determines that a message recipient is within its Internet domain but cannot find the user in NDS, the NMAP Agent modifies the domain portion of the address with the value placed in this field and requeues the message.

Specify the host name or IP address of a server designated to receive messages that are undeliverable within the local NIMS system. If you specify an IP address rather than a host name, you must enclose the IP address in square brackets [] to form a valid email address.

This option is a vital part of setting up a standalone messaging server. See [“Hub-and-Spoke Messaging System” on page 52](#).

Another important use of this option is to enable NIMS to share a domain name with another email system, for example, GroupWise. When this option is configured, the NMAP Agent forwards messages that belong to the domain but are not addressed to users within the NIMS messaging system. In the case of GroupWise, the destination server would be running a GroupWise Internet Agent.

Remote Queue Restrictions

This feature is designed for countries where users must pay a per use line fee. Using this option, you can restrict remote message delivery to non-peak hours.

Click Do Not Process Remote Queue to control when remote messages can be passed to the SMTP Agent for delivery across the Internet. In the Weekdays field, specify a time span, using the 24-hour clock, when the NMAP Agent will not process outgoing messages on Monday through Friday. In the Weekends field, do the same for Saturday and Sunday.

NMAP Agent: Context

Only users whose User objects are located in listed contexts have mailboxes in the NIMS system. The NMAP Agent requires local access to all User objects within its assigned context.

One NDS context for users is identified when you create the NMAP Agent object. You can add multiple user contexts on the Context page. Because

NMAP contexts are not inherited, every container or sub-container serviced by an NMAP Agent must be individually added to that agent's context list.

Messaging services will automatically be provided to every user in the specified context. Mailboxes will be created in the local message store directory the first time when users log in and receive messages.

In addition to the standard NIMS disk space requirements described in [“Initial NIMS Installation” on page 11](#), you must calculate an additional 3 KB on the SYS: volume for every NDS User object in the NMAP Agent's context because NDS requires 3 KB per User object replicated on the server.

Browse to and select one or more contexts for the NMAP Agent to service.

NMAP contexts are actually managed by the messaging server. When it starts, the messaging server generates a list of NMAP contexts and holds it in server memory for fast user lookups. The context list cannot be updated in memory; it can only be re-created. Consequently, if you add or remove contexts in the NMAP Agent configuration, the changes will not take effect until the messaging server is restarted. In distributed environments, every messaging server must be restarted.

The POP, IMAP, WebMail, Address Book, SMTP, AutoReply, Alias, Proxy and Finger Agents reference the context list when performing user-related functions.

NMAP Agent: Mailbox Quota

The system administrator can restrict the amount of disk space that user mailboxes are allowed to occupy by enabling mailbox quotas.

Mailbox Quota

Select Per User if you want to control mailbox size on an individual user basis. To set each individual mailbox quota, go to the Novell IMS Configuration page of each User object and specify that user's quota. See [“Configuring User Objects” on page 127](#)

Select System Wide if you want to establish a system default mailbox size.

If you select both Per User and System Wide, you can use the System Wide setting as the default and then adjust individual users' quotas up or down as needed. Individual user quotas override the system quota default.

Quota Return Message

Provide a standard reply for a sender whose message could not be delivered because the recipient's mailbox had already reached its maximum size.

NMAP Agent: Single Copy Message Store

The Single Copy Message Store (SCMS) feature allows the NMAP Agent to store email messages sent to multiple recipients in a shared location on the messaging server. By default, messages sent to two or more users and exceeding 2 KB in size are stored in the SCMS directory. A message must exceed both thresholds to be stored in the SCMS directory. For more information, see [“Single Copy Message Store Directory” on page 152](#).

Without SCMS, each recipient would receive a copy of every message in his or her own mailbox. Long messages and large attachments sent to multiple recipients would then rapidly consume large amounts of disk space.

Specify the minimum number of recipients for which individual copies of the same message will be stored.

Specify the minimum size in kilobytes of messages (including attachments) that should be stored in the SCMS directory.

NMAP Agent: Trusted Hosts

Although trusted host relationships are not required, they can be set up in distributed systems to improve performance. Without the trusted host relationship, agent hosts are forced to authenticate to the NMAP Agent in order to communicate with it (this authentication does not use clear-text passwords). The message store and message queue can be accessed, modified, or deleted by applications running on trusted hosts.

IMPORTANT:

Trusted Clients of this NMAP Server

Type the IP address of each server hosting NIMS agents that need open access to the NMAP Agent > click Add to add it to the list of trusted hosts.

On NetWare, 127.0.0.0 and localhost are automatically trusted hosts and do not need to be added to the list.

To delete an IP address from the list, select it > click Remove.

NMAP Agent: Clients

Each NIMS agent that interacts with an NMAP Agent is a client of that NMAP Agent. The Clients page lists all NIMS agents that are registered to the current NMAP Agent. It is an informational page; you cannot add or delete agents from the list.

SMTP Agent

NIMS supports Simple Mail Transfer Protocol (SMTP), a protocol used by email clients to send messages and by mail servers to exchange messages. The SMTP Agent is the means by which messages enter and leave your NIMS system across the Internet. The SMTP Agent must be running on at least one messaging server in the network in order for users to send messages across the Internet.

- ♦ [“Creating an SMTP Agent Object” on page 78](#)
- ♦ [“Configuring the SMTP Agent” on page 79](#)

For an illustration of how the SMTP Agent works, see [“Message Processing in the Message Queue” on page 154](#).

Creating an SMTP Agent Object

A Messaging Server container can hold only one SMTP Agent object. If you did not choose to create an SMTP Agent object during installation, you can add one later.

To create an SMTP Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add an SMTP Agent > click Create.
- 2** Double-click SMTP Agent.
- 3** Fill in the required fields:

Specify the Internet domain used by your organization. By default, the SMTP Agent's domain corresponds with the messaging server's official domain as configured on the Messaging Server object's Identification page. The SMTP Agent uses this domain to identify which messages belong to the local messaging system. Messages not belonging to the local system are routed over the Internet to their respective domains.

Browse to and select the NMAP Agent where the SMTP Agent should drop off messages.

- 4** Click Create to create the SMTP Agent object.
- 5** If you created the new SMTP Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 6** Continue with [“Configuring the SMTP Agent” on page 79](#).

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring the SMTP Agent

To configure the SMTP Agent using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object > right-click the SMTP Agent to configure > click Details.
- 2** Click a Details page > configure the SMTP Agent for your NIMS system needs.

Details Page	Options
--------------	---------

-
- 3** After configuring the SMTP Agent, click OK to save the changes.
 - 4** You may need to manually restart the SMTP Agent. See [“Restarting Individual Agents” on page 142.](#)
 - 5** Return to [“Configuring NIMS Objects and Agents” on page 61](#) to select a different NIMS agent to configure.

or

When you have configured all your NIMS agents, continue with [Chapter 4, “Optimizing Your NIMS Messaging Servers,” on page 115](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29.](#)

SMTP Agent: Identification

You must add all the domain and host names for which your NIMS system will accept messages in one of the two domain lists. Be aware of the following important points:

- ♦ No domain should ever be listed in both the Global Domain list *and* in the Hosted Domain list. Names added to both lists create ambiguities within the system.
- ♦ Failure to add all domain and host names that resolve to the server's IP address can result in 100% server utilization. Messages addressed to the overlooked domains are relayed instead of accepted; the missing name resolves to the server's IP address and the server relays the message to itself in an endless loop. NIMS will prevent such loops only for domains that resolve to loopback or the server's default IP address.

Names added to these lists will not be recognized until the SMTP Agent is restarted.

Place domain names in the Global Domain list if you want NIMS to remove the domain portion of the email address before looking up the user in NDS. Consequently, the portion of the email address to the left of the @ must be unique in the entire system. Users created without their domains included in their NDS object names can be addressed at all of the listed global domains.

For example, messages addressed to Bob@Novell.com and Bob@Novell.edu will be delivered to the same mailbox if Novell.com and Novell.edu are listed as Global Domains and an NDS object named Bob exists in one of the contexts assigned to an NMAP Agent. See [“NMAP Agent: Context” on page 75](#).

Place domain names in the Hosted Domain list if you want NIMS to use the entire email address when looking up the user in NDS. Consequently, the portion of the email address to the left of the @ does not need to be unique in the system. Users created with domains included in their NDS object names can only be addressed at the included domain.

For example, messages addressed to Bob@Novell.com and Bob@Novell.edu will be delivered to different mailboxes if Novell.com and Novell.edu are listed as Hosted Domains and NDS objects named Bob@Novell.com and Bob@Novell.edu exist in any one of the contexts assigned to an NMAP Agent. See [“NMAP Agent: Context” on page 75](#).

If you want to limit the size of messages that users can send, select the limit in the Message Size Limit field. You can select an amount between None (no limit) and 40 MB.

SMTP Agent: Options

Flags

The Flags section lists a series of standard SMTP commands that can be supported on the current SMTP Agent. Select the commands you want the SMTP Agent to accept.

The VRFY command allows external clients to verify that a user exists in your messaging system. If enabled, VRFY can pose a security risk because it allows external users to anonymously request verification of user names. For example, if spammers want to find out the user names in your company, they could query the system with a series of user names until the system verified a valid user name.

When verifying that a user exists in the messaging system, the SMTP Agent references the context list maintained by the messaging server. See [“NMAP Agent: Context” on page 75](#).

The EXPN command expands a group name upon request and lists all the user names in that group. This command is also considered a security risk because it allows spammers to anonymously request group membership lists. For example, if a spammer requests to expand a system-wide group such as Everyone, the SMTP Agent will return the complete membership list which is, essentially, every user name in your organization.

By default, the SMTP Agent accepts all incoming messages and places them in a queue for address verification processing as resources are available. This facilitates rapid message processing. If you want the SMTP Agent to perform address verification before accepting messages into your NIMS system, select Verify Addresses on Receipt.

The SEND ETRN command requests a remote server to send any messages it has queued for your messaging system. This option is primarily for organizations with dial-up Internet connections.

The ACCEPT ETRN command allows a remote server to request queued messages. If enabled, the SMTP Agent responds to this request by sending any messages it has queued for that system. ACCEPT ETRN is the only SMTP flag that is selected by default.

Mail Relay Host [Forwarder]

A mail relay host is a relay point for remote messages. It is often used to transfer messages out through a firewall.

Select Use Relay Host to funnel all remote messages through another SMTP Agent rather than having the current SMTP Agent access the Internet. Specify the host name or IP address of the SMTP server that will function as the mail relay host. All remote messages going through this SMTP Agent will then be forwarded to the SMTP Agent running at the designated address.

SMTP Agent: UBE Blocking

Flags

You can protect your NIMS system from UBE (unsolicited bulk email) or SPAM mail by blocking specified sites.

Restricts access to your NIMS system by selectively denying access. If this option is selected, the SMTP Agent refuses connections from any host with an IP address designated in the Blocked Hosts list. The Blocked Hosts list is defined below.

Provides reverse DNS lookups. When receiving messages from external systems, the SMTP Agent verifies that the sender's IP address has a corresponding host name published in DNS. If it doesn't, the SMTP Agent drops the connection.

Your DNS server must be configured to support reverse DNS lookups for this option to function.

Enables the SMTP Agent to do lookups on the Real-Time Black Hole List (RBL). RBL maintains a list of confirmed spammers and open relays. Specify the host name of the RBL list.

Blocked Hosts

Provide a list of blocked IP address ranges.

Type a range of disallowed IP addresses > click Add to add the disallowed range to the list. For example:

251.70.2.53-251.70.2.60

Repeat for each additional range of disallowed IP addresses. If you are using WebAdmin, be sure to provide only one range per line.

If Block Hosts in Blocked List is selected above, any hosts that fall within the designated IP address ranges will not be granted connections to the current SMTP Agent.

To delete a range of IP addresses from the list, select the range > click Delete.

SMTP Agent: UBE Relaying

You can keep your NIMS system from relaying UBE (unsolicited bulk email) or SPAM messages.

Flags

Prohibits users from sending remote messages through the SMTP Agent until they have first authenticated with the NIMS system by way of their POP3 or IMAP4 client within a designated time frame. This works for most Internet email clients because email clients always check for email (log in) just before sending messages. This option requires that you run the Connection Manager to perform the user authentication. See **“Connection Manager” on page 110**.

Enables Extended SMTP (ESMTP) authentication. If selected, the email client must authenticate through the ESMTP protocol before the SMTP Agent will relay messages to remote recipients. Netscape Communicator* and Outlook* Express support ESMTP authentication or an allowed list.

When authenticating users for sending remote messages, the SMTP Agent references the context list maintained by the messaging server. See **“NMAP Agent: Context” on page 75**.

Restricts access to your NIMS system by selectively allowing access. If this options is selected, only mail hosts with an IP address designated in the Allowed Hosts list can relay remote messages through this SMTP Agent. The Allowed Hosts list is defined below.

If SMTP-after-POP, ESMTP authentication, or the allowed list are all enabled, they function as an either/or option. If an email client does not authenticate by way of POP when downloading mail, it must authenticate by way of ESMTP or the allowed list before it can send remote messages.

Restricts the number of users who can receive the same message. The SMTP Agent only accepts the first *n* recipients. You can also configure the WebMail Agent to restrict the number of recipients per email. See [“WebMail Agent: Configuration” on page 90](#).

Allowed Hosts

Provide a list of allowed IP address ranges. If an ISP or corporation has its own Web server, listing the organization’s range of registered IP addresses prevents external hosts, such as spammers, from relaying messages through the company’s messaging system.

Type a range of allowed IP addresses > click Add to add the allowed range to the list. For example:

251.70.2.53-251.70.2.60

Repeat for each additional range of allowed IP addresses. If you are using WebAdmin, be sure to provide only one range per line.

If Require Sender to Be in Allowed List for Remote Sending is selected above, hosts that fall within the designated IP address ranges will be allowed to address remote recipients.

To delete a range of IP addresses from the list, select the range > click Delete.

POP Agent

NIMS supports Post Office Protocol 3 (POP3). The POP Agent provides access to the NIMS system for users with any POP3 email client.

In addition to the basic memory requirements described in [“Initial NIMS Installation” on page 11](#), the POP Agent requires approximately 200 KB per expected simultaneous connection to your NIMS system.

For an illustration of how the POP Agent services POP3 email clients, see [“POP3 Client Request for Messages” on page 156](#).

Creating a POP Agent Object

A Messaging Server container can hold only one POP Agent object. If you did not choose to create a POP Agent object during installation, you can add one later.

To create a POP Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add a POP Agent > click Create.
- 2** Double-click POP Agent.
- 3** Click Create to create the POP Agent object.
- 4** If you created the new POP Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 5** Provide POP3 email client users with the information they need to access their NIMS mailboxes. See [“Configuring a POP3 or IMAP4 Email Client” on page 121](#).

When logging users into the messaging system, the POP Agent references the context list maintained by the messaging server. See [“NMAP Agent: Context” on page 75](#). When a user logs in by way of POP, the POP Agent passes the username to the messaging server. If the username exists within the context list, the username is authenticated using the password and the user can download his or her messages. If the username does not appear in the context list, the user is denied access to the messaging system.

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

IMAP Agent

NIMS supports Internet Mail Access Protocol 4 (IMAP4). The IMAP Agent provides access to the NIMS system for users with any IMAP4 email client.

In addition to the basic memory requirements provided in [“Initial NIMS Installation” on page 11](#), the IMAP Agent requires approximately 300 KB per expected simultaneous connection to your NIMS system.

For an illustration of the IMAP Agent services IMAP4 email clients, see [“IMAP4 Client Request for Messages” on page 157](#).

Creating an IMAP Agent Object

A Messaging Server container can hold only one IMAP Agent object. If you did not choose to create an IMAP Agent object during installation, you can add one later.

To create an IMAP Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add an IMAP Agent > click Create.
- 2** Double-click IMAP Agent.
- 3** Click Create to create the IMAP Agent object.
- 4** If you created the new IMAP Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 5** Provide IMAP4 email client users with the information they need to access their NIMS mailboxes. See [“Configuring a POP3 or IMAP4 Email Client” on page 121](#).

When logging users into the messaging system, the IMAP Agent references the context list maintained by the messaging server. See [“NMAP Agent: Context” on page 75](#). When a user logs in by way of IMAP, the IMAP Agent passes the username to the messaging server. If the username exists within the context list, the username is authenticated using the password and the user can download or send messages. If the username does not appear in the context list, the user is denied access to the messaging system.

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

WebMail Agent

The WebMail Agent provides the browser-based interface for users to send and receive messages, manage their folders, and set mail preferences from a Web browser.

In addition to the basic memory requirements provided in [“Initial NIMS Installation” on page 11](#), the WebMail Agent requires 300 KB per expected simultaneous connection to your NIMS system.

- ♦ [“Creating a WebMail Agent Object” on page 88](#)
- ♦ [“Configuring the WebMail Agent” on page 89](#)

For an illustration of how the WebMail Agent interacts with a Web browser, see [“WebMail Client Request for Messages” on page 158](#).

Creating a WebMail Agent Object

A Messaging Server container can hold only one WebMail Agent object. If you did not choose to create a WebMail Agent object during installation, you can add one later.

To create a WebMail Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add a WebMail Agent > click Create.
- 2** Double-click WebMail Agent.
- 3** Browse to and select the NMAP Agent with which the WebMail Agent should communicate.
- 4** Click Create to create the WebMail Agent object.
- 5** If you created the new WebMail Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 6** Continue with [“Configuring the WebMail Agent” on page 89](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring the WebMail Agent

To configure the WebMail Agent using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object > right-click the WebMail Agent > click Details.
- 2** Click a Details page > configure the WebMail Agent for your NIMS system needs.

Details Page	Options
--------------	---------

-
- 3** After configuring the WebMail Agent, click OK to save the changes.
 - 4** You may need to manually restart the WebMail Agent. See “[Restarting Individual Agents](#)” on page 142.

- 5 Provide WebMail client users with the information they need to access their NIMS mailboxes. See [“Using the NIMS WebMail Client” on page 122](#).

When logging users into the messaging system, the WebMail Agent references the context list maintained by the messaging server. See [“NMAP Agent: Context” on page 75](#). When a user logs in by way of WebMail, the WebMail Agent passes the username to the messaging server. If the username exists within the context list, the username is authenticated using the password and the user can view his or her messages. If the username does not appear in the context list, the user is denied access to the messaging system.

- 6 Return to [“Configuring NIMS Objects and Agents” on page 61](#) to select a different NIMS agent to configure.

or

When you have configured all your NIMS agents, continue with [Chapter 4, “Optimizing Your NIMS Messaging Servers,” on page 115](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

WebMail Agent: Configuration

Type the title you want to appear in the WebMail client title bar.

Displays the port numbers the WebMail client will use for HTTP and SSL. The default HTTP port is 80. The default SSL port is 443. Use the default port numbers unless that port number is already in use by another program on the server.

In the Type field, select the location where you want the advertising frame to appear on the WebMail page > in the URL field, type the URL to the page you want to display.

If you want to limit aspects of users' messages, specify the maximum size limit for outgoing messages and the maximum number of recipients allowed for a single message. You can also restrict the maximum number of recipients when configuring the SMTP Agent. See [“SMTP Agent: UBE Relaying” on page 84](#).

WebMail does not restrict the size of inbound messages it downloads from the user's mailbox.

WebMail Agent: Interface

Specify the number of messages to display on the WebMail client Message List page.

Select the default language for the WebMail interface.

Select Allow Change if you want users to be able to change their own passwords. Because NIMS is completely integrated with NDS, the WebMail client password is the same as the user's NetWare login password. Therefore, selecting this option on the WebMail Agent's Interface page actually gives your users rights to their NetWare login password through WebMail, regardless of whether they have rights to the actual password property in their NDS User object.

Select Require SSL if you want the WebMail Agent to require an SSL connection with the WebMail client before users can change their passwords.

Select Hide Compose so users cannot send messages.

By default, all configurable WebMail features are selected and therefore configurable by users. Deselect Allow Preference Changes if you do not want users to be able to configure options in WebMail Preferences. If you do not allow users to configure their own Preferences settings, you can configure preferences for them on User objects. See [“Configuring User Objects” on page 127](#).

Select Preferences Only if users are not using the WebMail client for sending and receiving messages but you still want them to be able to configure NIMS features like autoreply and forwarding using the WebMail Preferences page. In addition, when you terminate user accounts, you can select Only Configuration to keep the terminated users from retrieving messages from your server, but still allow them to set up forwarding functions that will forward their messages to their new email accounts.

Places the user's Reply To address in the From field of messages. This option is only valid when a user defines a Reply-To address in the WebMail client Preferences. If Use Reply-To as From Address is not selected here, the user's From field will display their *user_name@official_domain*.

When the WebMail Agent is extremely busy, it can redirect WebMail access requests to another WebMail agent. Select Redirect to URL if Busy to turn on redirection.

Specify the URL of another server where a WebMail Agent is running, for example, `http://127.5.4.1/`. If the WebMail Agent on that server is running on a port other than the default port of 80, supply the port number as well, for example, `http://127.5.4.1:88/`. If you chain your WebMail Agents into a circle, WebMail access requests are redirected until an available WebMail Agent is discovered.

WebMail Agent: Appearance

You can change the default colors used in the WebMail client and its online help.

Colors

You can change foreground and background colors of five page areas:

Any space not occupied by other, more specific elements. The page background is gray by default.

The area at the top and bottom of the page, where the page title and buttons are located. The border background is lavender by default.

A main heading. The heading background is gray by default.

A type of information you provide or that is listed for you. The field name background is blue by default.

The area where you specify field values. The field body background is beige by default.

If you want to experiment with various color schemes, you will find it easier to work in the WebMail client, where you can test your color settings immediately. After deciding on a color scheme, set the colors on the WebMail Agent Appearance page to establish the default colors for all WebMail users. Individual WebMail users may then customize the colors for the WebMail interface in WebMail Preferences. Values set in WebMail Preferences override the defaults set for the WebMail Agent on a system level.

WebMail Agent: Address Book

You can control what kind of Address Book information is available to WebMail client users.

Select Enabled so WebMail client users can look up email addresses in the WebMail Address Book.

Select Personal to allow users to create their own personal address books. A user's personal address book is stored in his or her NDS user object. Consequently, the user can access the personal address book from any location as long as the user is logged in to the network.

Specify the maximum number of entries allowed in personal address books. The options are 25, 50, or 100 entries. This setting enables you to manage the disk space required by the user's personal address book.

Select System-Wide to allow users access to the system Address Book that contains all NIMS users. In the LDAP Server field, provide the IP address or host name of the LDAP server where the Address Book Agent runs. In the Context field, specify the domain name you are interested in. If the Context field is left blank, all domain names are returned. Users found in any domain are searched.

Users with the Privacy preference set to Limited or None in WebMail Preferences are visible to other NIMS users in the system-wide Address Book. Users with the Privacy preference set to Unlisted are not visible in the system-wide Address Book.

Select Public to allow users access to a public LDAP directory service. If desired, specify the IP address or host name of the LDAP server to use as the default public directory. In the Context field, specify the domain name you are interested in. If the Context field is left blank, all domain names are returned.

Address Book Agent

The Address Book Agent provides address book information using read-only LDAP access to NDS. By communicating with the Address Book Agent, any LDAP-compliant application can access address book information in NDS. For example, the Address Book feature of WebMail uses the Address Book Agent to query NDS for address book information.

To speed up LDAP queries, the Address Book Agent maintains an index of all users in its supported NDS contexts. When queried, the Address Book Agent references its index file to identify the user's context. Once it identifies the user's context, the Address Book Agent locates the user's address book information in NDS. Because the Address Book Agent directly references NDS for user information, its information is always as current as NDS.

In addition to providing LDAP access to NDS, the Address Book Agent can generate an address book file. This LDIF file can be used to distribute address

book information to messaging systems, such as remote sites, that do not have access to the Address Book Agent.

The information revealed about each user in the Address Book depends on the user's privacy level. See [“Using WebMail for User Self-Administration” on page 123](#).

- ♦ [“Creating an Address Book Agent Object” on page 94](#)
- ♦ [“Configuring the Address Book Agent” on page 95](#)
- ♦ [“Filtering the Results of Address Book Lookups” on page 96](#)

Creating an Address Book Agent Object

A Messaging Server container can hold only one Address Book Agent object. If you did not choose to create an Address Book Agent object during installation, you can add one later.

To create an Address Book Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add an Address Book Agent > click Create.
- 2** Double-click Address Book Agent.
- 3** Browse to and select an NMAP Agent whose contexts will be available for address book queries.

You can select only one NMAP Agent when creating the Address Book Agent object. You can select additional NMAP Agents when configuring the Address Book Agent.

- 4** Click Create to create the Address Book Agent object.
- 5** If you created the new Address Book Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 6** Continue with [“Configuring the Address Book Agent” on page 95](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring the Address Book Agent

To configure the Address Book Agent using NetWare Administrator:

- 1 Browse to and double-click the Messaging Server object > right-click the Address Book Agent > click Details.
- 2 Click a Details page > configure the Address Book Agent for your NIMS system needs.

Details Page	Options
--------------	---------

-
- 3 After configuring the Address Book Agent, click OK to save the changes.
 - 4 You may need to manually restart the Address Book Agent. See [“Restarting Individual Agents” on page 142](#).
 - 5 Return to [“Configuring NIMS Objects and Agents” on page 61](#) to select a different NIMS agent to configure.

or

When you have configured all your NIMS agents, continue with [Chapter 4, “Optimizing Your NIMS Messaging Servers,” on page 115](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Address Book Agent: Configuration

Scheduler

Specify how many days should elapse between re-creations of the address book index. The default is 1 day. The maximum setting is 99 days.

While the Address Book Agent's user index enables faster user lookups, it is not dynamically regenerated. If a new user object is added to NDS, the Address Book Agent will not be able to find that user until its user index is regenerated.

LDAP/LDIF

Select **Enable LDAP Lookup Server on Port** to enable LDAP lookups > specify the port number the Address Book Agent should use to listen for client requests for address book information. The default port number is 389.

Select **Enable Automatic LDIF File Export** if you need the address book information in LDIF format every time the Address Book index is regenerated. LDIF stands for LDAP Data Interchange Format, which allows other programs to make use of the information in the NIMS Address Book.

- ♦ On NetWare, the ADDRBOOK.LDF file is created in the SYS:\PUBLIC directory.
- ♦ On Solaris and Linux, the `addrbook.ldf` file is created in the `/usr/bin` directory.

Filtering the Results of Address Book Lookups

If your NIMS system includes multiple hosted systems, you probably do not want the Address Book Agent to return all matches when the Address Book Agent searches the system-wide address book. You only want it to return the matches found in that user's hosted system. To isolate hosted systems from each other for address book searches, you can configure Organization and Organizational Unit container objects with specific domain names.

To associate an Organization or Organizational Unit object with a particular domain name:

- 1** Browse to and right-click the container object > click **Details**.
- 2** Click **Novell IMS Options**.
- 3** In the **Domain** field, specify the domain name to associate with the container.
- 4** Click **OK** to save the setting.
- 5** Restart the NMAP Agent and Address Book Agent that service the modified context. See **“Restarting Individual Agents” on page 142**.

AutoReply Agent

The AutoReply Agent lets users create a custom message that is automatically sent in response to new messages received. For example, when users go on vacation, they can create a custom message that lets others know that they're unavailable.

In addition, the AutoReply Agent provides forwarding capabilities to let users specify an alternate email address where incoming messages will be automatically forwarded. This is useful to users who may have a second email address where they want copies of their messages sent on a regular basis.

The AutoReply Agent can also forward SMS messages to cellular phones and pagers. It does not configure SMS messages; it recognizes SMS messages and forwards them to cellular phones and pagers.

The AutoReply Agent is not email-client specific. Although users configure mail forwarding and autoreply messages in WebMail, the AutoReply Agent functions independently of any email client. Therefore, NIMS can handle forwarding and autoreply messages for users of POP3, IMAP4, and WebMail clients.

For an illustration of how the AutoReply Agent works, see [“Message Processing in the Message Queue” on page 154](#).

Creating an AutoReply Agent Object

A Messaging Server container can hold only one AutoReply Agent object. If you did not choose to create an AutoReply Agent object during installation, you can add one later.

To create an AutoReply Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add an AutoReply Agent > click Create.
- 2** Double-click AutoReply Agent.
- 3** Browse to and select an NMAP Agent with which the AutoReply Agent should communicate.
- 4** Click Create to create the AutoReply Agent object.
- 5** If you created the new AutoReply Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Rule Agent

The Rule Agent executes rules defined in the WebMail client. See the online help in the WebMail client for information about rules.

For an illustration of how the Rule Agent works, see [“Message Processing in the Message Queue” on page 154](#).

Creating a Rule Agent Object

A Messaging Server container can hold only one Rule Agent object.

To create a Rule Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add a Rule Agent > click Create.
- 2** Double-click Rule Agent.
- 3** Browse to and select the NMAP Agent with which the Rule Agent should communicate.
- 4** Click Create to create the Rule Agent object.
- 5** If you created the new Rule Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 6** Notify users that they can now set up rules to automate message handling in their mailboxes using the WebMail client. See [“Using the NIMS WebMail Client” on page 122](#).

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Proxy Agent

The Proxy Agent lets users retrieve messages from up to three additional POP3 or IMAP4 email accounts and consolidate them into their NIMS mailbox. In this way, users can manage several email accounts from a central mailbox.

The Proxy Agent cannot retrieve email from mail systems that do not provide POP3 or IMAP4 access to their users' mailboxes.

- ♦ [“Creating a Proxy Agent Object” on page 99](#)
- ♦ [“Configuring the Proxy Agent” on page 100](#)

For an illustration of how the Proxy Agent works, see [“Proxy Request to Download Messages” on page 159](#).

Creating a Proxy Agent Object

A Messaging Server container can hold only one Proxy Agent object. If you did not choose to create a Proxy Agent object during installation, you can add one later.

To create a Proxy Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add a Proxy Agent > click Create.
- 2** Double-click Proxy Agent.
- 3** Select an NMAP Agent to designate the message queue into which the Proxy Agent can insert messages.
- 4** Click Create to create the Proxy Agent object.
- 5** If you created the new Proxy Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 6** Continue with [“Configuring the Proxy Agent” on page 100](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring the Proxy Agent

To configure the Proxy Agent using NetWare Administrator:

- 1 Browse to and double-click the Messaging Server object > right-click the Proxy Agent > click Details.
- 2 Click a Details page > configure the Proxy Agent for your NIMS system needs.

Details Page	Options
--------------	---------

- 3 After configuring the Proxy Agent, click OK to save the changes.
- 4 You may need to manually restart the Proxy Agent. See “Restarting Individual Agents” on page 142.
- 5 Return to “Configuring NIMS Objects and Agents” on page 61 to select a different NIMS agent to configure.

or

When you have configured all your NIMS agents, continue with Chapter 4, “Optimizing Your NIMS Messaging Servers,” on page 115

You can also perform this procedure using WebAdmin. For more information, see “Using WebAdmin” on page 29.

Proxy Agent: Configuration

Select how many hours you want to elapse between each message retrieval cycle. The default is 3 hours.

Select how many Proxy Agent threads you want to use to retrieve messages simultaneously. The more threads, the faster the message retrieval, but additional threads consume additional server memory. The default is 1 thread.

Alias Agent

The Alias Agent provides flexibility in email address format. You can define aliases automatically or manually. The automatic aliasing feature pulls information directly from NDS to generate aliases for NDS user objects. For example, a user named Steve Jones could receive messages addressed to Steve_Jones, Steve.Jones, SJones, and so on. Manually defined aliases can correspond to any Internet email address, perhaps based on function, such as `feedback@company.com`. Then you can designate actual users who should receive messages addressed to the special user names.

The aliases set up for the Alias Agent are not defined as Alias objects in NDS. They are maintained by the Alias Agent and are specific to your NIMS messaging system.

- ♦ [“Creating an Alias Agent Object” on page 101](#)
- ♦ [“Configuring the Alias Agent” on page 102](#)

For an illustration of how the Alias Agent works, see [“Message Processing in the Message Queue” on page 154](#).

Existing NDS aliases are automatically recognized by NIMS. Because these aliases are defined in NDS, they function independently of the Alias Agent. Messages addressed to these aliases are automatically delivered to the associated User object’s mailbox. No Alias Agent is needed when an NDS alias exists.

Creating an Alias Agent Object

A Messaging Server container can hold only one Alias Agent object. If you did not choose to create an Alias Agent object during installation, you can add one later.

To create an Alias Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add an Alias Agent > click Create.
- 2** Double-click Alias Agent.
- 3** Browse to and select an NMAP Agent whose contexts the Alias Agent can generate user aliases for.

You can select only one NMAP Agent when creating the Alias Agent object. You can select additional NMAP Agents when configuring the Alias Agent.

- 4** Click Create to create the Alias Agent object.
- 5** If you created the new Alias Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 6** Continue with [“Configuring the Alias Agent” on page 102](#).

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring the Alias Agent

To configure the Alias Agent using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object > right-click the Alias Agent > click Details.
- 2** Click a Details page > configure the Alias Agent for your NIMS system needs.

Details Page	Options
--------------	---------

- 3** After configuring the Alias Agent, click OK to save the changes.
- 4** You may need to manually restart the Alias Agent. See “Restarting Individual Agents” on page 142.
- 5** Return to “Configuring NIMS Objects and Agents” on page 61 to select a different NIMS agent to configure.

When you have configured all your NIMS agents, continue with **Chapter 4, “Optimizing Your NIMS Messaging Servers,”** on page 115

Format	Example
--------	---------

The Fullname formats only work if you enter users' full names in the Full Name field of their User objects.

Automatically generated aliases are considered local aliases.

Alias Agent: Local Aliases

Local aliases are applied only to messages passing through the local Alias Agent's monitored queue. For local aliases, the Alias Agent uses its own alias table. Local aliases are ideal when you are maintaining identical aliases, such as Admin or Postmaster, on multiple messaging servers.

To build a local alias table, type an alias in the left field > type the corresponding user name or IP address in the right field > click Add.

If the replacement string is an IP address, the IP address must be enclosed in square brackets [].

If the replacement string is a username, the domain name portion of the user's email address is omitted. The replacement string cannot include the user's full email address because the domain portion of the email address is typically stripped out by the SMTP Agent before the message enters the queue. The only instance in which the SMTP Agent does not strip out the domain portion of the email address is when the address belongs to a hosted domain. Therefore, if the user belongs to a hosted domain, the replacement string must include both the username and the domain portion of the user's email address. For more information on hosted domains, see [“SMTP Agent: Identification” on page 80](#).

The alias appears in the list using the following syntax:

alias = user_name

For example, if a user's user name were SJones and he wanted to be known also by SteveJ, you would enter:

SteveJ = SJones

Users could then address email to SteveJ and it would be delivered to SJones' mailbox.

You could also set up a local alias such as feedback@company.com that would automatically go to whomever you specify in the local alias. The destination can be either a local or remote email address.

When you are finished entering aliases, click OK to create the local alias table.

If you encounter problems with the aliases you have defined, see [“Messages Addressed to an Alias Are Not Delivered” on page 164](#) for assistance.

To delete an alias, select it > click Remove.

To create a large number of aliases, you can type them into an ASCII text file, then import them. Use the format illustrated above, with <CR><LF> between lines. Click Import > browse to and select the ASCII file of aliases > click OK.

Alias Agent: Global Aliases

Global aliases are applied to messages passing through the monitored queues of all Alias Agents in your NIMS system. For global aliases, all Alias Agents search a shared alias table that includes entries contributed by Alias Agents throughout your NIMS system. Global aliases are preferred for user-specific aliases.

Other than the fact that global aliases are universally recognized throughout the message system, there is no difference between local and global aliases. Global aliases are defined in exactly the same manner as local aliases and the same rules apply. See [“Alias Agent: Local Aliases” on page 104](#) for details.

AntiSpam Agent

The AntiSpam Agent allows the Postmaster or NIMS administrator to build a blackout list of undesirable email domains and addresses. Messages sent from domains and email addresses contained in the blackout list will not be accepted into your NIMS system.

- ♦ [“Creating an AntiSpam Agent Object” on page 105](#)
- ♦ [“Configuring the AntiSpam Agent” on page 106](#)

For an illustration of how the AntiSpam Agent works, see [“Message Processing in the Message Queue” on page 154](#).

Creating an AntiSpam Agent Object

A Messaging Server container can hold only one AntiSpam Agent object. If you did not choose to create an AntiSpam Agent object during installation, you can add one later.

To create an AntiSpam Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add an AntiSpam Agent > click Create.
- 2** Double-click AntiSpam Agent.
- 3** Browse to and select an NMAP Agent with which the AntiSpam Agent should communicate.

You can select only one NMAP Agent when creating the AntiSpam Agent object. You can select additional NMAP Agents when configuring the AntiSpam Agent.

- 4** Click Create to create the AntiSpam Agent object.
- 5** If you created the new AntiSpam Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 6** Continue with [“Configuring the AntiSpam Agent” on page 106](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring the AntiSpam Agent

To configure the AntiSpam Agent using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object > right-click the AntiSpam Agent > click Details.
- 2** Click a Details page > configure the AntiSpam Agent for your NIMS system needs.

Details Page	Options

- 3** After configuring the AntiSpam Agent, click OK to save the changes.
- 4** You may need to manually restart the AntiSpam Agent. See [“Restarting Individual Agents” on page 142.](#)
- 5** Return to [“Configuring NIMS Objects and Agents” on page 61](#) to select a different NIMS agent to configure.

or

When you have finished configuring all your NIMS agents, continue with [Chapter 4, “Optimizing Your NIMS Messaging Servers,” on page 115](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29.](#)

AntiSpam Agent: Configuration

Blocked Domains and Addresses

In the Blocked Sites box, specify the domain (for example, *company.com*) or email address (for example, *Joe@company.com*) to block > click Add. If you enter a domain name, all email addresses ending with that domain name are blocked. If you enter a specific email address, only that exact address is blocked. Repeat this process until you have entered all the desired domains and/or addresses, one per line.

To delete a domain or address, select it > click Remove.

To block a large number of domains and addresses, you can type them into an ASCII text file, then import them. Use the format illustrated above, with <CR><LF> between lines. Click Import > browse to and select the ASCII file of domains and addresses to block > click OK.

Send Back

Select Send Back if you want messages from blocked sites to be returned to the senders.

CC Postmaster

Select CC Postmaster if you want the Postmaster to receive copies of messages from blocked sites.

List Agent

The List Agent provides list server functionality and NDS mailing lists in your NIMS system. See [Chapter 6, “Managing NIMS Users,” on page 127](#) for instructions on setting up these services for your NIMS users.

- ♦ [“Creating a List Agent Object” on page 108](#)
- ♦ [“Configuring the List Agent” on page 108](#)

For an illustration of how the List Agent works, see [“Message Processing in the Message Queue” on page 154](#).

Creating a List Agent Object

A Messaging Server container can hold only one List Agent object.

To create a List Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add a List Agent > click Create.
- 2** Double-click List Agent.
- 3** Browse to and select an NMAP Agent with which the List Agent should communicate
- 4** Click Create to create the List Agent object.
- 5** If you created the new List Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 6** Continue with [“Configuring the List Agent” on page 108](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring the List Agent

To configure the NMAP Agent using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object > right-click the NMAP Agent to configure > click Details.

- 2 Click a Details page > configure the NMAP Agent for your NIMS system needs.

Details Page	Options
--------------	---------

- 3 After configuring the List Agent, click OK to save the changes.
- 4 You may need to manually restart the List Agent. See [“Restarting Individual Agents” on page 142.](#)
- 5 Set up mailing lists or list servers for your users. See [“Setting Up NDS Mailing Lists” on page 130](#) and [“Setting Up a List Server” on page 132.](#)
- 6 Return to [“Configuring NIMS Objects and Agents” on page 61](#) to select a different NIMS agent to configure.

or

When you have configured all your NIMS agents, continue with [Chapter 4, “Optimizing Your NIMS Messaging Servers,” on page 115](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29.](#)

List Agent: Configuration

You can schedule when you want the List Agent to perform its list server functions:

Specify the time, using the 24-hour clock, when you want the List Agent to create its daily digest of list server activity.

Finger Agent

Finger is an Internet utility. The Finger Agent lets a finger client anywhere find out information about friends and colleagues by retrieving information from user profiles. Given an email address, the Finger Agent returns the user's full name and any other information the user has chosen to supply. Given a

first or last name, the Finger Agent also returns the login names of users whose first or last names match.

WebMail users can specify a message or other information they want returned when another user fingers their email address. See [“User: Finger Configuration” on page 130](#).

On Solaris and Linux, NIMS uses the Finger daemon for this functionality.

Creating a Finger Agent Object

A Messaging Server container can hold only one Finger Agent object. If you did not choose to create a Finger Agent object during installation, you can add one later.

To create a Finger Agent object using NetWare Administrator:

- 1** Browse to and right-click the Messaging Server object where you want to add a Finger Agent > click Create.
- 2** Double-click Finger Agent.
- 3** Click Create to create the Finger Agent object.
- 4** If you created the new Finger Agent on Solaris or Linux, you must restart your NIMS system to start the new agent. See [“Startup Commands” on page 137](#).

NetWare Administrator can automatically start new agents on NetWare servers.

- 5** Notify users that fingering capabilities are now available.

When allowing users to be fingered, the Finger Agent references the context list maintained by the messaging server. See [“NMAP Agent: Context” on page 75](#).

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Connection Manager

The Connection Manager provides user authentication services by tracking the IP addresses of client users. The POP, IMAP, and SMTP Agents can all make use of the Connection Manager’s services.

Shared Agent Functions

Multiple NIMS agents share the following Details pages:

- ♦ [“Queue Server” on page 112](#)
- ♦ [“Monitored Queues” on page 112](#)
- ♦ [“Monitored Servers” on page 113](#)
- ♦ [“Status” on page 113](#)

Queue Server

The NMAP Agent functions as the message queue server. It manages messages entering and leaving its message queue. The Queue Server page is available for the Proxy Agent, the SMTP Agent, and the WebMail Agent because these agents insert messages into the message queue managed by the NMAP Agent.

Select an NMAP Agent > click OK so the current agent will insert messages into the message queue belonging to the selected NMAP Agent.

If a queue agent is not running on the same server as the NMAP Agent, the queue agent server can be a trusted host of the NMAP Agent server for faster access. See [“NMAP Agent: Trusted Hosts” on page 77](#).

Monitored Queues

The Monitored Queues page is available for the AntiSpam Agent, the AutoReply Agent, the Rules Agent, and the SMTP Agent. Each agent monitors a specific message queue through an NMAP Agent, and processes messages that are placed in that queue.

Browse to and select one or more NMAP Agents > click OK so the current agent starts monitoring its message queue through the selected NMAP Agents.

For an illustration of how the queue agents process messages, see [“Message Processing in the Message Queue” on page 154](#).

Monitored Servers

The Monitored Servers page is available for the Address Book Agent, the Alias Agent, and the Proxy Agent because these agents need to access one or more message stores through NMAP Agents.

Browse to and select one or more NMAP Agents > click OK so the current agent will start monitoring the selected NMAP Agents.

Status

The Status page is available for all NIMS agents.

By default, the agent is enabled. Select Disable Agent > click OK to disable the current agent.

- ♦ For NetWare, NetWare Administrator stops the NLM agents immediately. As long as its status is Disabled, the agent will not restart if you restart the rest of the NIMS system.
- ♦ For Solaris and Linux, NetWare Administrator cannot stop the agents automatically. You must stop them manually. See [“Restarting Individual Agents” on page 142](#).

4

Optimizing Your NIMS Messaging Servers

NIMS is a high-performance messaging system. Make sure each messaging server is optimized to accommodate NIMS capabilities:

- ♦ “Optimizing a NetWare Server for NIMS” on page 115
- ♦ “Optimizing a Solaris Server for NIMS” on page 119
- ♦ “Optimizing a Linux Server for NIMS” on page 119

Optimizing a NetWare Server for NIMS

You can optimize the performance of NIMS by modifying your NetWare® server configuration.

- ♦ “Starting the Console Monitor” on page 116
- ♦ “Modifying the Communications Parameters” on page 116
- ♦ “Modifying Directory Caching Parameters” on page 116
- ♦ “Modifying File Caching Parameters” on page 117
- ♦ “Modifying File System Parameters” on page 118
- ♦ “Exiting the Console Monitor” on page 118
- ♦ “Restarting Your NetWare Server” on page 118

The recommended value settings described in the steps are dependent on the amount of memory available to your system. Depending on the amount of available memory, you might need to use slightly lower values.

For example, if you have 256 MB or more of memory available, use the recommended values. If you have less than 256 MB, use lower values. If you receive memory errors, the values are set too high.

Starting the Console Monitor

To start the Console Monitor to modify server parameters:

- 1 Type **load monitor** at the console prompt.
- 2 In the Available Options box, select **Server Parameters** > press Enter to display the **Select a Parameter Category** box.

You may need to scroll to the bottom of the list to find Server Parameters.

Modifying the Communications Parameters

To allow for high load email traffic, you must adjust the Minimum and Maximum Packet Receive Buffers settings to optimize the speed performance of NIMS.

In the Select a Parameter Category box:

- 1** Select Communications > press Enter.
- 2** Modify each parameter listed in the table below as indicated:

File Caching Parameter	Set To

- 3** Press Esc to exit the Communications Parameters box and return to the Select a Parameter Category box.

Modifying Directory Caching Parameters

To maximize the performance of NIMS with NDS[®], you must adjust directory caching parameters.

In the Select a Parameter Category box:

- 1** Select Directory Caching > press Enter.

- 2 Modify each parameter listed in the table below as indicated:

Cache Parameter	Set To
-----------------	--------

- 3 Press Esc to exit the Directory Caching Parameters box and return to the Select a Parameter Category box.

Modifying File Caching Parameters

Modifying file caching parameters allows better file system performance.

In the Select a Parameter Category box:

- 1 Select File Caching > press Enter.
- 2 Modify each parameter listed in the table below as indicated:

File Caching Parameter	Set To
------------------------	--------

- 3 Press Esc to exit the File Caching Parameters box and return to the Select a Parameter Category box.

Modifying File System Parameters

Modifying file system parameters allows faster server startup time and improves the performance of the NIMS message store. However, you will lose the ability to restore deleted files on your volume.

In the Select a Parameter Category box

- 1** Select File System > press Enter.
- 2** Select Immediate Purge of Deleted Files > press Enter to change the setting to On.
- 3** Press Esc to exit the File System Parameters box and return to the Select a Parameter Category box.
- 4** Exit the Console Monitor by pressing Esc twice and pressing Enter.

Exiting the Console Monitor

- 1** Press Esc to exit the Select a Parameter Category box.
- 2** Press Esc to exit the Available Options box.
- 3** Press Alt+F10 > select yes > press Enter to exit the Console Monitor.

Restarting Your NetWare Server

In order for the changes to take effect, you must down and then restart your server.

At the console prompt:

- 1** Type **down** > press Enter.
- 2** Once the server is down, type **server** at the DOS prompt to restart it.

Optimizing a Solaris Server for NIMS

On Solaris*, the types of optimization described in “[Optimizing a NetWare Server for NIMS](#)” on page 115 are done automatically by the NIMS programs. No manual optimization is required for NIMS to run efficiently on Solaris.

Optimizing a Linux Server for NIMS

On Linux*, the NIMS programs optimize performance in the same way that is described in “[Optimizing a NetWare Server for NIMS](#)” on page 115. You may be able to get further operating system optimization; consult your Linux documentation for more information.

5

Configuring Email Clients for Use with NIMS

Many Internet email clients are available. It is easy to configure them to work with NIMS.

- ♦ [“Configuring a POP3 or IMAP4 Email Client” on page 121](#)
- ♦ [“Using the NIMS WebMail Client” on page 122](#)
- ♦ [“Using WebMail for User Self-Administration” on page 123](#)

Configuring a POP3 or IMAP4 Email Client

Because Outlook* Express can be configured as either a POP3 or an IMAP4 email client, it is used as an example below.

For information on configuring other email clients such as Netscape Communicator* or Eudora*, refer to the email client’s configuration guide and contact your system administrator for the host names of your client protocol and SMTP servers.

To configure Outlook Express to send and receive email via NIMS:

- 1** Start Outlook Express.
- 2** If you already have an existing Outlook Express account, click Tools > Accounts > Add > Select Mail to start the Internet Connection Wizard.
The Internet Connection Wizard prompts you for your name.
- 3** Type your name as you would like it to display on your messages > click Next.
- 4** Type your email address > click Next.

- 5** From the list box, select POP or IMAP.
- 6** In the Incoming Mail Server field, type the host name of the server where the POP or IMAP Agent is running.
- 7** In the Outgoing Mail Server field, type the host name of the server where the SMTP Agent is running.

Depending on the configuration of your NIMS system, the incoming mail server and outgoing mail server may be the same messaging server or different messaging servers.

- 8** Click Next.
- 9** Enter your POP or IMAP account name and password > click Next.
- 10** Enter a Friendly Name for your Outlook Express mail account.
- 11** Select your connection type and click Next.
- 12** Click Finish.

Now you can use Outlook Express to send and receive messages through NIMS.

For an illustration of how POP3 and IMAP4 email clients interact with your NIMS system, see “[POP3 Client Request for Messages](#)” on page 156 and “[IMAP4 Client Request for Messages](#)” on page 157.

Using the NIMS WebMail Client

WebMail is a Web-based client that allows users to send and receive messages from anywhere if they are connected to the Internet and have a Web browser.

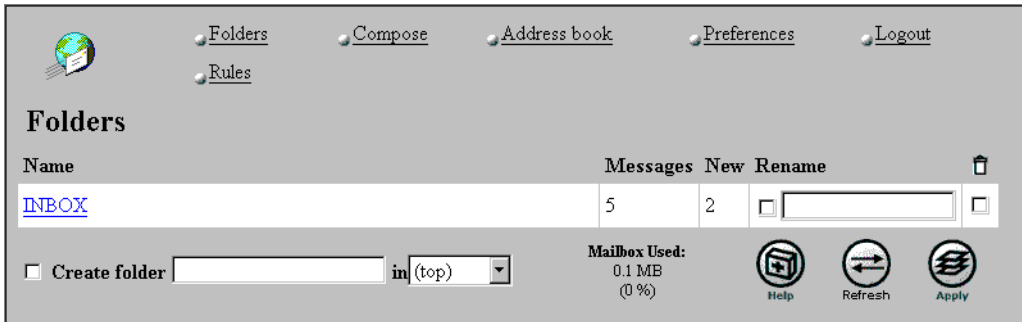
To use WebMail:

- 1** In your Web browser, enter the URL or host name of the server where NIMS is installed.

If the WebMail Agent is using the default port number of 80, you do not need to specify it. If you are using a different port number, you must specify the port number along with the URL or host name. For example:

`http://127.5.4.1:88/`
`http://quickmail:88/`

- 2** Enter your username and password to display the WebMail client.



3 Click Compose to write a message.

or

Click Preferences to configure the WebMail client.

Click Help on any page for additional instructions.

For an illustration of how WebMail interacts with your NIMS system, see [“WebMail Client Request for Messages” on page 158.](#)

Using WebMail for User Self-Administration

One of the advantages of NIMS is that users can perform many self-administration tasks by setting WebMail Preferences, even if they are using POP3 or IMAP4 email clients. These self-administration features are managed by NIMS and can only be configured in the WebMail client, not in the POP3 or IMAP4 email clients. In addition, WebMail Preferences enable users to configure email capabilities that may not be available in the POP3 or IMAP4 email clients.

Explain the following steps to users of POP3 and IMAP4 email clients if you want them to use WebMail for self-administration:

1 Start the WebMail client as explained in [“Using the NIMS WebMail Client” on page 122.](#)

2 Click Preferences.

You as system administrator can make various options available in the Preferences page, depending on how you configure the WebMail Agent. See [“WebMail Agent: Interface” on page 91.](#)

Users can use the online help available in the Preferences page of WebMail to learn how to set their preferences.

The following preferences affect capabilities available to POP3 and IMAP4 email client users:

- ♦ “General Settings” on page 124
- ♦ “Password” on page 125
- ♦ “Forwarding” on page 125
- ♦ “Auto-Reply/Vacation Message” on page 125
- ♦ “Finger Daemon” on page 125
- ♦ “Proxy Configuration” on page 125

General Settings

You can allow users to customize the functionality of their NIMS mailboxes.

Users can choose how much personal information they want to share with other NIMS users in the Address Book.

- ♦ All NIMS users will have access to other users’ first and last names, email addresses, and phone numbers if this information is stored in NDS®.

All NIMS users will have access only to other users’ email addresses.

None of the personal information will be available.

Users can choose how long they remain logged into WebMail during a period of inactivity. After the specified time limit has passed, users are automatically logged out to maintain the security of their mailboxes.

If users don't want replies to their messages sent to their WebMail mailboxes, they can specify a different email address that will be used automatically when recipients reply to their messages.

If the sending email client includes encoding information, WebMail translates messages into the UTF-8 character set. If WebMail cannot determine the encoding scheme of an incoming message, it uses the character set the user selects.

Password

This option allows users to change their passwords without having to contact their system administrator or ISP. To change the password, users must enter the old password once and then enter the new password twice. The new password will be required the next time they log in to WebMail.

Changing the WebMail password actually changes users' network login password. Therefore, the new password will also be required the next time they log in to the network.

If users do not see the Password preference, see [“Password Preference Is Not Available in WebMail Preferences” on page 163](#) for assistance.

Forwarding

NIMS recognizes that users may have multiple email identities and locations. Users can configure NIMS to automatically send their messages wherever they want to receive them. Users can choose whether or not they want to keep a local copy.

Auto-Reply/Vacation Message

NIMS recognizes that occasionally users will not be retrieving messages for an extended period of time, such as while attending a professional conference or taking a vacation. Users can configure NIMS to reply to messages while they are away.

Finger Daemon

Users can provide the information they want to send to users who use a finger client to find out about them.

Proxy Configuration

If users have additional email accounts, they can set up NIMS to routinely retrieve messages from the other accounts. For example, if a user has email accounts at work, home, and school, he or she can specify the addresses and the client will copy any new messages from them to your NIMS mailbox.

6

Managing NIMS Users

Because of NDS[®], you do not need to create separate NIMS user accounts in order for your users to begin exchanging messages. However, you can customize the services you provide to users:

- ♦ “Configuring User Objects” on page 127
- ♦ “Setting Up NDS Mailing Lists” on page 130
- ♦ “Setting Up a List Server” on page 132
- ♦ “Creating Local Message Stores for User Contexts” on page 136

Configuring User Objects

If you grant users self-administration privileges, users can configure most of these settings for themselves. See “Using WebMail for User Self-Administration” on page 123.

If you do not grant users self-administration privileges, you can configure individual User objects or groups of User objects.

To configure a user using NetWare[®] Administrator:

- 1** Browse to and right-click the User object > click Details.

If you select multiple users, only a subset of the User object properties can be edited.

- 2** Click a Details page > configure the mailing list for your list server needs.

-
- 3** Click OK to save the user configuration.

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

User: Configuration

General

Select a level of privacy for the user:

- ♦ All NIMS users will have access to the user’s first and last name, email address, and phone number if this information is stored in NDS.
- ♦ All NIMS users will have access only to the user’s email address.
- ♦ None of the user’s personal information will be available.

Enter the number of minutes until automatic timeout. After the specified time limit has passed, the user is automatically logged out to maintain mailbox security.

Specify a preferred reply-to email address if you don't want replies to the user's messages sent to the user's WebMail mailbox.

If this field is left blank, the default email address is *user_name@official_domain*. If a container domain has been established, the default email address is *user_name@container_domain*.

Forwarding

Select Forward Mail To > type the email address where you want to forward the user's messages.

Select Keep Local Copy if you want to retain copies of the user's messages in the user's mailbox.

AutoReply/Vacation

Select Reply to All Received Mail with Message > type the message to use as a response while the user is away.

Store

By default, the user's access to his or her mailbox is enabled. Select User Disabled to remove the user's access to his or her mailbox. Messages to a disabled user are considered undeliverable when they arrive in the NIMS system.

Selecting this option does not disable the User object in NDS; it only removes the User object from the messaging system.

Select Disk Quota > specify the maximum mailbox size in kilobytes to restrict the size of the user's mailbox. For this to take effect, you must also select the Per User option on the Mailbox Quota page of the NMAP Agent object. See [“NMAP Agent: Mailbox Quota” on page 76](#).

This setting can be used to allocate additional mailbox space to system administrators, the messaging server's Postmaster, or high level executives. It overrides the system-wide disk quota set when you configure the NMAP Agent.

User: Proxy Configuration

NIMS allows you to set from 1 to 3 specific proxy configurations for each user.

The options on this page do not work unless the Proxy Agent is enabled for the current NMAP context. See [“Proxy Agent” on page 99](#).

Select which proxy entry you want to create.

Select POP3 or IMAP4.

Select Leave Mail on Server if you want copies of message left in the other email mailbox.

Provide the host name of your service provider's POP or IMAP server.

This is not simply the name of the service provider. For example, the user has an account with a service provider named ABCMail. The host is not "ABCMail." It will probably be something like `imap.abcmail.com` or `mail.abcmail.com`. If you do not know the host name, contact your service provider.

Provide the user name for the other email account.

Provide the password for the other email account.

Click Clear to clear the entry.

User: Finger Configuration

Type the response you want NIMS to send if this user is fingered from another system. For more information, see [“Finger Agent” on page 109](#).

Setting Up NDS Mailing Lists

An NDS mailing list allows you to send messages to all users located in one or more NDS container objects (such as an Organization, Organizational Unit, Group, Role, or User).

- ♦ [“Creating an NDS Mailing List” on page 131](#)
- ♦ [“Configuring an NDS Mailing List” on page 131](#)

Creating an NDS Mailing List

To create an NDS Mailing List object using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object where you want to add an NDS mailing list > right-click Mailing Lists > click Create.
- 2** Double-click NDS List.
- 3** Fill in the required fields:

Type a unique name for the NDS Mailing List object.

Browse to and select the NMAP Agent you want to service the NDS mailing list.

- 4** Click Create to create the NDS Mailing List object.
- 5** Continue with [“Configuring an NDS Mailing List” on page 131](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring an NDS Mailing List

To configure an NDS mailing list using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object > double-click the Mailing Lists object > right-click the NDS Mailing List object > click Details.
- 2** Click a Details page > configure the mailing list for your list server needs.

Details Page	Options
--------------	---------

-
- 3** Click OK to save the NDS mailing list configuration.

- 4 Notify the users selected in the Senders field that the NDS mailing list is available for use.

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

NDS Mailing List: Configuration

General

Type an abstract of the NDS mailing list.

Type a description of the NDS mailing list.

Select one or more users who are authorized to send to this NDS mailing list.

Select one or more NDS container objects whose users will comprise the NDS mailing list.

Options

Select Require Sender to Authenticate via SMTP to ensure that the user sending a message to the NDS mailing list is authorized to use the list.

NDS Mailing List: NMAP Store

Select the NMAP Agent associated with the message store where you want to store the mailing list.

Setting Up a List Server

The List Agent provides list server functionality in your NIMS system. The Mailing List object holds the names of the users that have subscribed to the list server.

- ♦ [“Creating a Mailing List for a List Server” on page 133](#)
- ♦ [“Configuring a Mailing List for a List Server” on page 133](#)

Creating a Mailing List for a List Server

To create a Mailing List object using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object where you want to add a mailing list for a list server > right-click Mailing Lists > click Create.
- 2** Double-click List.
- 3** Fill in the required fields:

Type a unique name for the Mailing List object.

Remember that list names must be different from user names within the system.

Browse to and select the NMAP Agent you want to service the mailing list.

- 4** Click Create to create the Mailing List object.
- 5** Continue with [“Configuring a Mailing List for a List Server” on page 133](#)

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Configuring a Mailing List for a List Server

To configure a mailing list for a list server using NetWare Administrator:

- 1** Browse to and double-click the Messaging Server object > double-click the Mailing Lists object > right-click the Mailing List object to configure > click Details.
- 2** Click a Details page > configure the mailing list for your list server needs.

3 Click OK to save the mailing list configuration.

4 Notify users that the list server is available.

Users can use the following commands to subscribe the list server, select list server services, and unsubscribe from the list server:

Command	Description
<i>list_name</i>	
<i>list_name</i>	
<i>list_name options</i>	
<i>list_name</i>	
<i>list_name</i>	
<i>list_name</i>	

Command	Description
<i>list_name</i>	
<i>list_name</i>	

Users should address messages containing commands to ListServ@domain.com. Commands must be placed in the *body* of the message, *not* in the subject line.

You can also perform this procedure using WebAdmin. For more information, see [“Using WebAdmin” on page 29](#).

Mailing List: Configuration

General

Type a description of the mailing list that will be included in the welcome message returned to users when they subscribe to the list.

Type a description of the mailing list for internal use.

Type the fully distinguished names of one or more users to serve as moderators of the list.

Options

Select Invitation Only so users must apply to a list moderator for membership.

Select Open so that anyone can post to the mailing list at any time, whether he or she is subscribed or not.

Select Plaintext Signatures to turn on use of the plain text signature defined on the Signatures page.

Select HTML Signatures to turn on use of the HTML signature defined on the Signatures page.

Select Block Attachments if you do not want users to include attachments with their messages. Messages with attachments will be bounced.

Select Keep Archive if you want the List Agent to archive all activity in this mailing list.

Select Allow Digest if you want users to be able to subscribe to a digest rather than receiving all messages individually.

Mailing List: Signatures

You can set up standard text that will be appended automatically to every message sent by the list server.

Type a message to append to plain text messages.

Type a message to append to HTML messages. It can include HTML codes.

Mailing List: NMAP Store

Select the NMAP Agent associated with the message store where you want to store the mailing list.

Creating Local Message Stores for User Contexts

A single NMAP Agent can service users in many contexts. An initial message store is created when you configure the NMAP Agent. However, it may be convenient to set up additional message stores that are local to the users. You can set up separate message stores based on users' Organization and Organizational Unit container objects. It is important to set up separate message stores *before* users start sending messages.

To set up a separate, local message store:

- 1** Browse to and right-click the container object > click Details.
- 2** Click Novell IMS Options.
- 3** In the Message Store field, specify the location where you want to create the message store.
- 4** Click OK to save the setting.
- 5** Restart the NMAP Agent that services the modified context. See [“Restarting Individual Agents” on page 142](#)

The mailbox directory structure for users in this context is created at the new location you specified.

A

NIMS Commands and Utilities

NIMS includes various commands and utilities that are used to manage the messaging server and provide statistical information. The commands and utilities are critical in maintaining and troubleshooting a NIMS system.

- ♦ “Startup Commands” on page 137
- ♦ “NetWare Console Commands” on page 144
- ♦ “Server Utilities” on page 147

Startup Commands

- ♦ “NetWare Startup Commands” on page 137
- ♦ “Solaris Startup Commands” on page 139
- ♦ “Linux Startup Commands” on page 140
- ♦ “Restarting Individual Agents” on page 142

NetWare Startup Commands

NIMS startup commands load applications on the server. The startup NLM programs are located in the SYS:\SYSTEM directory.

- ♦ “MSGSRV Startup Command” on page 138
- ♦ “IMS Startup Command” on page 138
- ♦ “WEBADMIN Startup Command and Switches” on page 138

MSGSRV Startup Command

MSGSRV starts the messaging server and its associated client protocol and queue agents. It goes through NDS[®] and reads the messaging server configuration and the names of the agents associated with the Messaging Server object to determine which NLM programs to load.

To load the messaging server, type **load msgsrv** at the console prompt.

To unload the messaging server, type **unload msgsrv** at the console prompt. This command unloads the messaging server and its associated agents.

Because NDS takes some time to initialize after startup, do not use the MSGSRV command in the AUTOEXEC.NCF file. If MSGSRV.NLM is loaded before NDS has completed its initialization process, it will not be able to reference NDS for information on the messaging server's configuration and which agents to load. Therefore, the messaging server will fail to load. Use the IMS command instead.

IMS Startup Command

IMS verifies that NDS is loaded before launching MSGSRV. Because IMS waits for NDS to load before launching the messaging server, it is recommended that you use IMS to start your messaging server, particularly in the AUTOEXEC.NCF.

To launch the messaging server, type **load ims** at the console prompt.

- ♦ To unload the messaging server on a NetWare 5.x server, type **ims unload**.
- ♦ On a NetWare 4.1x server, use **load ims unload**.

The IMS command does not load or unload the WebAdmin Agent or the MAILCON utility. If WebAdmin or MAILCON are running on the server, they must be manually unloaded at the console before unloading the messaging server.

WEBADMIN Startup Command and Switches

WEBADMIN loads the WebAdmin Agent on the messaging server so the WebAdmin administration tool can be accessed from a workstation browser. For information on accessing the WebAdmin utility, see [“Using WebAdmin” on page 29](#)

The following switches can be used with the WEBADMIN command:

Switch	Description
<i>port</i>	
<i>SSL_port</i>	

Solaris Startup Commands

nims Script

On Solaris*, the NIMS software is installed in `/opt/NOVLnims` and its subdirectories. The NIMS startup script on Solaris is `/etc/init.d/nims`. Use `/etc/init.d/nims start` and `/etc/init.d/nims stop` to start and stop NIMS.

ims Executable

The `nims` script includes running the `/opt/NOVLnims/bin/ims` executable, which functions as a monitor and auto-loader for your NIMS system. It keeps track of the agents that should be running and restarts them if needed.

The following switches can be used with the `ims` executable either in the `nims` script or on the command line:

Switch	Description
<i>core_directory</i>	
	<i>time</i>
	<i>agent_name</i>

Switch	Description
	<i>seconds</i>
	<i>email_address SMTP_server</i>

The following kill commands can be used with `ims`:

Command	Description
<code>pkill -15 ims</code>	<code>ims</code>
<code>pkill -16 ims</code>	<code>pkill -15</code>
<code>pkill -17 ims</code>	<code>ims</code>

Linux Startup Commands

nims Script

On Linux*, the NIMS software is installed in `/usr/local/nims` and its subdirectories. The NIMS startup script on Linux is `/etc/rc.d/init.d/nims`. Use `/etc/rc.d/init.d/nims start` and `/etc/rc.d/init.d/nims stop` to start and stop NIMS.

ims Executable

The `nims` script includes running the `/usr/local/nims/bin/ims` executable, which functions as a monitor and auto-loader for your NIMS system. It keeps track of the agents that should be running and restarts them if needed.

The following switches can be used with the `ims` executable either in the `nims` script or on the command line:

Switch	Description
<i>core_directory</i>	<i>time</i>
	<i>agent_name</i>
<i>seconds</i>	
<i>email_address</i>	<i>SMTP_server</i>

The following kill commands can be used with `ims`:

Command	Description
<code>killall -15 ims</code>	<code>ims</code>
<code>killall -10 ims</code>	<code>killall -15</code>
<code>killall -12 ims</code>	<code>ims</code>









Restarting Individual Agents







- ♦ “On NetWare” on page 142
- ♦ “On Solaris and Linux” on page 143

On NetWare

Whenever you modify the configuration of an agent using NetWare® Administrator, NetWare Administrator automatically restarts the modified agent. However, WebAdmin does not automatically start or restart modified agents. Therefore, you must start or restart them manually.

To restart an individual agent, use the UNLOAD command to stop it, then use the LOAD command to restart it.




Agent Object	Agent Name	NLM Program
		
		
		
		
		
		
		
		










Agent Object	Agent Name	NLM Program
		
		
		
		
		
		

On Solaris and Linux

On Solaris and Linux, neither NetWare Administrator nor WebAdmin can automatically restart modified agents. To restart an individual agent, kill that agent's process. The NIMS autoloader then notices that a required agent is not running and restarts it for you.

- ♦ On Solaris, use `pkill -9 agent_module_name`
- ♦ On Linux, use `killall -9 agent_module_name`

Agent Object	Agent Name	Module Name
		
		
		

Agent Object	Agent Name	Module Name
		
		
		
		
		
		
		
		
		
		
		

NetWare Console Commands

The console commands perform a single function at the command line. The console NLM programs are located in the SYS:\SYSTEM directory.

- ♦ “SYSLOG Commands” on page 145
- ♦ “MAIL Commands” on page 145

SYSLOG Commands

The Syslog provides logging and report capabilities that you can use to diagnose problems and fine-tune server performance. For more information about the Syslog, see [“Internet Services” on page 63](#).

- ♦ [“SYSLOG CONFIG” on page 145](#)
- ♦ [“SYSLOG FLUSH” on page 145](#)

SYSLOG CONFIG

SYSLOG CONFIG identifies what log level has been configured and the file names to which log messages are being written.

SYSLOG FLUSH

By default, the messaging server’s Syslog files are written to memory. If Log to File is marked in either the Internet Services or server object’s Syslog Configuration page, the messaging server continues to write the Syslog file to memory but intermittently flushes the log file to disk. The SYSLOG FLUSH command forces the messaging server to flush the log file in memory to disk.

MAIL Commands

The MAIL command provides monitoring and control of the message queue.

- ♦ [“MAIL STAT” on page 145](#)
- ♦ [“MAIL QUEUE” on page 146](#)
- ♦ [“MAIL REMOVE domain” on page 146](#)
- ♦ [“MAIL SPAM” on page 146](#)

See also [“MAILCON \(NetWare Only\)” on page 147](#).

MAIL STAT

MAIL STAT gives you a static snapshot of the messaging server’s statistics at a command prompt. You must enter the command again to update the statistics.

This command gives you the same statistics as the MAILCON utility and the total number of NMAP connections. The advantage of the MAIL STAT

command over the MAILCON utility is that it requires very few server resources.

MAIL QUEUE

MAIL QUEUE looks at the server's message queue and lists the target domains for outbound messages and the number of messages going to those domains.

This command is primarily a SPAM intervention option. If spammers are using your messaging server to relay or bounce SPAM, you will generally be inundated with messages going to one or two domains. Using this command, you can identify which domains are being hit.

You can then use the MAIL REMOVE command to delete those messages while they are still in the queue.

MAIL REMOVE *domain*

MAIL REMOVE removes all the queued messages that are going to the specified domain.

This command is used in conjunction with MAIL QUEUE to delete SPAM from your message queue.

MAIL SPAM

MAIL SPAM reports statistics that correspond to specific anti-SPAM features. Reported values are dependent on whether the associated properties are configured.

Reported statistics include:

- ♦ `bounced` corresponds to the Bounced Message Control option in the NMAP Agent's Parameters page. See "[NMAP Agent: Parameters](#)" on [page 73](#).
The reported value is the number of bounced messages that have been deleted. Values will depend on the NMAP Agent's bounced message threshold.
- ♦ `blocked` corresponds to the Do Not Allow Access from Hosts in Blocked List option in the SMTP Agent's UBE Blocking page. See "[SMTP Agent: UBE Blocking](#)" on [page 83](#).

The reported value is the number of hosts in the SMTP Agent's blocked hosts list that have attempted to connect with the current messaging server.

- ♦ [\[blank\]](#) corresponds to the Check Against RBL List at Server option in the SMTP Agent's UBE Blocking page. See ["SMTP Agent: UBE Blocking" on page 83](#)

The reported value is the number of hosts on the RBL list that have attempted to connect with the current messaging server.

- ♦ [\[blank\]](#) corresponds to the Require Sender To Be in the Allowed List for Remote Sending option in the SMTP Agent's UBE Relaying page. See ["SMTP Agent: UBE Relaying" on page 84](#).

The reported value is the number of hosts not included in the SMTP Agent's Allowed hosts list that have attempted to send remote messages.

- ♦ [\[blank\]](#) corresponds to the Deny Access to Hosts Not in DNS option in the SMTP Agent's UBE Blocking page. See ["SMTP Agent: UBE Blocking" on page 83](#)

The reported value is the number of hosts without valid DNS entries that have attempted to connect with the current messaging server.

Server Utilities

The server utilities are programs that can be run from the messaging server.

- ♦ ["MAILCON \(NetWare Only\)" on page 147](#)
- ♦ ["IMSAUDIT \(NetWare Only\)" on page 148](#)
- ♦ ["NIMSEXT" on page 149](#)

MAILCON (NetWare Only)

The MAILCON utility is used to monitor a messaging server's performance. Using the Available Options menu, you can select which server you want to monitor, set monitoring options, open the Statistics Details window, or exit the program.

The Statistics Details window provides much of the same information available in the messaging server object's Status tab. It displays:

- ♦ The number of local and remote messages that have been queued, received and delivered
- ♦ The total number of recipients of inbound and outbound messages
- ♦ The total number of client connections; that is, the number of people logged in at that moment through the POP, IMAP, or WebMail Agents
- ♦ The total number of server connections; that is, the number of users and other messaging servers that are sending SMTP or WebMail messages to the messaging server for processing in the message queue
- ♦ The volume of inbound and outbound mail processed by the messaging server
- ♦ Server uptime

The MAILCON utility does not report the total number of NMAP connections. That statistic is only available through the MAIL STAT command. See “MAIL STAT” on page 145.

In addition to the basic statistics reported in the messaging server’s Status page, the MAILCON utility displays:

- ♦ The number of failed messages
- ♦ The number of wrong passwords entered
- ♦ The number of unauthorized NMAP connections

Under Monitoring Options, you can configure the Statistics window to update every minute, every second, or every 10 seconds.

IMSAUDIT (NetWare Only)

IMSAUDIT counts the total number of people who have logged into the messaging system. This utility allows administrators to determine the total number of NIMS mailboxes on their messaging system. Disabled users or users who have never logged in are not counted.

This utility is made available for customers who are leasing NIMS licenses on a monthly, per-user basis. To get a complete record of user mailboxes, IMSAudit needs to be run on every server running the NMAP Agent (that is every server that has a message store). The utility creates the log file SYS:\ETC\IMSAUDIT.LOG.

NIMSEXT

The NIMSEXT utility can be used to add or remove the NIMS schema from NDS. NIMSEXT is used by the installation program to extend the NDS schema during initial installation.

IMPORTANT:

To uninstall NIMS, you must run NIMSEXT to remove the NIMS schema. See “[Administrator Wants to Uninstall NIMS](#)” on page 168

On Solaris and Linux, use `nimsext .sh`.

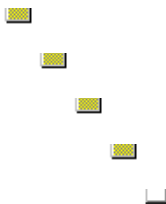
B

NIMS Directory Structure and Message Processing


By understanding the internal structure of your NIMS system and how messages are processed through it, you can more easily troubleshoot problems should they arise.


- ♦ “Message Store Directory” on page 151
- ♦ “Single Copy Message Store Directory” on page 152
- ♦ “Message Queue Directory” on page 153
- ♦ “Message Processing in the Message Queue” on page 154
- ♦ “POP3 Client Request for Messages” on page 156
- ♦ “IMAP4 Client Request for Messages” on page 157
- ♦ “WebMail Client Request for Messages” on page 158
- ♦ “Proxy Request to Download Messages” on page 159
- ♦ “Connection Manager User Authentication” on page 160

Message Store Directory







 *folder_name*

 *folder_name*

 *FOLDER_NAME*

 *folder_name*

 *folder_name*

More disk space is required to maintain directories on the messaging server than files. Consequently, sub-folders are very "expensive" in terms of server resources.

Single Copy Message Store Directory



 xxxx

 xxxx

xxxx

Message Queue Directory



└─ Cxxxxxxx

xxxxxxx

└─ xxxxxxxx

└─ Xxxxxxxx 000

└─ Xxxxxxxx 001

└─ Xxxxxxxx 002

└─ Xxxxxxxx 003

└─ Xxxxxxxx 004

└─ Xxxxxxxx 005







└─ Xxxxxxxx 006

└─ Xxxxxxxx 007

Message Processing in the Message Queue

The message queue processing described below includes all NIMS queue agents. If you have chosen not to run a particular queue agent, its step would be omitted from the described processing.




Stage	Icon	Description
-------	------	-------------







Stage	Icon	Description
6		
7	 	
8		
9		
10		

Stage	Icon	Description
8		<ul style="list-style-type: none">◆◆◆◆
9		

POP3 Client Request for Messages

The POP3 protocol is used to retrieve messages. When the POP Agent retrieves a message, it usually downloads the message to the local mail client and then deletes it from the user’s mailbox. Consequently, POP3 mail clients must store everything locally: user preferences, folders, and all retrieved messages. While POP3 conserves space on the messaging server, users can only access their folders and retrieved messages locally.



Stage	Icon	Description
1		
2		
3		








Stage	Icon	Description
4		
5		
6		
7		
8		
9		

IMAP4 Client Request for Messages





The IMAP4 protocol is capable of sending and receiving messages and it provides users with more versatility than the POP3 protocol. When the IMAP Agent retrieves a message, it downloads the message to the local mail client but leaves a copy of the message in the user's mailbox.






In fact, folders and messages are maintained on the messaging server. This means that users can access their folders and messages from any location. The drawback is that, unless restricted, mailbox growth can quickly consume the messaging server's disk space.

Stage	Icon	Description
1		
2		






Stage	Icon	Description
3		
4		
5		
6		
7		
8		
9		

WebMail Client Request for Messages








Stage	Icon	Description
1		
2		
3		
4		

Stage	Icon	Description
5		
6		
7		
8		
9		

Proxy Request to Download Messages

Stage	Icon	Description
1		
3		
4		
5		
6		

Connection Manager User Authentication

Stage	Icon	Description
1		
2		
3		
4		
5		
6		
7		

C

Troubleshooting

See “[Solving NIMS Problems](#)” on page 161 for a list of common NIMS problems and their solutions.

Solving NIMS Problems

- ♦ “[Users Cannot Send Internet Email](#)” on page 162
- ♦ “[Users Cannot Access the WebMail Client](#)” on page 162
- ♦ “[Users Have Duplicate User IDs](#)” on page 162
- ♦ “[Login Is Denied Because of Incorrect Password](#)” on page 163
- ♦ “[Password Preference Is Not Available in WebMail Preferences](#)” on page 163
- ♦ “[Mailboxes Are Damaged](#)” on page 163
- ♦ “[Messages Addressed to an Alias Are Not Delivered](#)” on page 164
- ♦ “[Incoming Mail Is Not Being Delivered on a Solaris or Linux System](#)” on page 166
- ♦ “[Messaging Server Shows High Utilization](#)” on page 166
- ♦ “[Distributed Messaging System Is Not Functioning](#)” on page 167
- ♦ “[Standalone Messaging System Can Send Messages to the WAN but Cannot Receive Them](#)” on page 167
- ♦ “[NIMS System Must Service Users in Multiple NDS Trees](#)” on page 167
- ♦ “[Administrator Wants to Uninstall NIMS](#)” on page 168

Users Cannot Send Internet Email

- Problem: The user cannot send Internet messages.
- Possible Cause: Port 25 may be in use by another SMTP application such as the GroupWise® Internet Agent. The Internet Agent or other SMTP applications cannot be run on a NIMS messaging server.
- Action: Unload the SMTP application > restart your NIMS system.

Users Cannot Access the WebMail Client

- Possible Cause: Several users cannot access the WebMail client. The WebMail Agent is running on the messaging server and other users apparently have no problem in accessing the client.
- Action: It is possible that the users' context has not been added as an NMAP Agent context. In this case, add the user's context to the NMAP Agent's context list. See **“NMAP Agent: Context” on page 75**. Restart the messaging server.
- Action: If the users' context has been added as an NMAP Agent context, restart the messaging server to ensure that the new context is recognized. See **“Startup Commands” on page 137**.
- Action: If the users' contexts are assigned to an NMAP Agent running on a standalone server, a WebMail Agent must be running locally on the standalone server.

Users Have Duplicate User IDs

- Problem: The current NDS® tree has duplicate user names in different containers.
- Possible Cause: All users belonging to a distributed messaging system must have unique user ID in order to access their mailboxes.
- The reason for this is that IMAP and POP clients do not supply the user's domain or context information (by RFC definition). They only provide the user ID. Given only the user ID, the IMAP, POP, and WebMail Agents must determine who is logging in. Where duplicate user IDs exist in different contexts, NIMS uses the first user it finds.
- It is possible to maintain duplicate user IDs on different standalone messaging servers.

Login Is Denied Because of Incorrect Password

- Problem:** The user is receiving Incorrect Password and Login Denied error messages.
- Possible Cause:** The user container is not registered as an NMAP context.
- Action:** To resolve the problem, add the container to the NMAP Agent's Context list. See **"NMAP Agent: Context" on page 75**. Restart the messaging server.
- If you do not want to register the entire container as an NMAP context, you can move the user to a supported context.

Password Preference Is Not Available in WebMail Preferences

- Problem:** A user accesses WebMail and cannot see the Password preference on the Preferences page.
- Possible Cause:** The user's ISP has not given him or her rights to change his or her password.
- Action:** The user can contact his or her ISP to see if password changing can be enabled.
- Possible Cause:** The user's ISP requires an SSL connection for password changes.
- Action:** If the user's ISP requires an SSL connection for password changes, the user must log in to his or her ISP using the Secure Sockets Layer (SSL) protocol.

The user can follow these steps to resolve the problem:

- 1** In your Web browser, type the letter **s** after **http** in your WebMail URL. For example:

`https://mail.company.com`

- 2** Press Enter.

- 3** When prompted, enter your username and password.

If you receive an error, you must contact your ISP to find out the port number to use for connecting using SSL.

Once the user can connect using SSL, the Password preference will now be available.

Mailboxes Are Damaged

- Problem:** POP, IMAP, or WebMail clients hang when retrieving messages.
- Possible Cause:** System instability can cause mailbox files to become corrupt.
- Action:** Determine which folder is hanging. If it is a POP user, the folder is always INBOX. Delete the folder's index file:

MAIL\USERS\user_name\folder_name.IDX. This file will be regenerated the next time the client tries to access the mailbox.

It may take awhile to regenerate the folder's index file if there are many messages.

Messages Addressed to an Alias Are Not Delivered

Problem: *NDS Aliases:*

Messages addressed to the name of an NDS alias object are delivered to the corresponding user object's mailbox.

Possible Cause: The alias object or the NDS object are not in one of the contexts serviced by NMAP.

Possible Cause: Synchronization problems in NDS.

Possible Cause: The alias object name or the user object name is not unique within the NMAP contexts.

Problem: *Automatically Created Aliases:*

These aliases are automatically generated by the Alias Agent from information stored in the NDS user objects. Automatically generated aliases are created as local aliases.

Possible Cause: The Alias Agent object has not been created. See [“Creating an Alias Agent Object” on page 101](#).

Possible Cause: The Automatically Create Aliases Using Information in the User Object option in the Alias Agent object is not selected. See [“Alias Agent: Configuration” on page 103](#).

Possible Cause: Synchronization problems in NDS.

Possible Cause: The alias is not unique. For example, if more than one user has the same Given and Last names, the Alias Agent will not be able to resolve First.Last aliases to one user.

Possible Cause: Your alias database is not being created. To verify this is the problem, go to the messaging server's Work directory. In the DBF (database files) subdirectory, you will see several *.BTR (Btrieve) files. These files should have today's date. If they do not have today's date, the alias database is not being regenerated, in which case contact Novell® Technical Services .

If any errors are generated in the alias database (such as duplicate aliases), the Alias Agent notes the conflict in the Syslog file and sends an SNMP trap (if you have SNMP configured).

Problem: *Local Aliases:*

A local alias is not working as intended. Local aliases are only recognized by the current Alias Agent. Local aliases are typically used in situations where identical aliases may be used on multiple messaging servers (such as postmaster, admin, or abuse). See [“Configuring the Alias Agent” on page 102](#) and [“Alias Agent: Local Aliases” on page 104](#).

Possible Cause: The Alias Agent object has not been created. See [“Creating an Alias Agent Object” on page 101](#)

Possible Cause: The replacement string does not correspond to a valid email address or NDS user. Check your alias tables. See [“Alias Agent: Local Aliases” on page 104](#) and [“Alias Agent: Global Aliases” on page 105](#).

Possible Cause: The alias or replacement string is not an exact match. Check your alias tables. See [“Alias Agent: Local Aliases” on page 104](#) and [“Alias Agent: Global Aliases” on page 105](#).

Possible Cause: More than one user corresponds to the replacement string. Check your alias tables. See [“Alias Agent: Local Aliases” on page 104](#) and [“Alias Agent: Global Aliases” on page 105](#).

Possible Cause: Synchronization problems in NDS.

Possible Cause: The replacement string cannot include the user’s full email address (*username@domain*) unless the user belongs to a hosted domain. This is because the domain portion of the email address is normally stripped out by the SMTP Agent before the message enters the queue.

Possible Cause: For users in hosted domains, the replacement string must match the user’s full email address (*username@domain*). This is because the SMTP Agent does not strip out the domain portion of the address for users in hosted domains. See [“SMTP Agent: Identification” on page 80](#).

Problem: *Global Aliases:*

A global alias is not working as intended. Global aliases are recognized by every Alias Agent in the message system. Global aliases are preferred for user-specific aliases.

Possible Cause: You can encounter the same problems with global aliases as you do with local aliases. See *Local Aliases* above. For more information about the Alias Agent, see [“Configuring the Alias Agent” on page 102](#).

Incoming Mail Is Not Being Delivered on a Solaris or Linux System

Problem: Incoming mail is not arriving.

Possible Cause: The SMTP Agent is unable to bind to port 25 because `sendmail` is running and is already using that port number. The SMTP Agent and `sendmail` cannot run on the same server.

Action: To tell if `sendmail` is running, type **`telnet localhost 25`** at a command prompt. If you receive a response similar to the following:

```
220 domain.com ESMTP Sendmail 8.9.3/8.8.7
```

then `sendmail` is running.

To stop `sendmail` on Solaris*, type **`/etc/init.d/sendmail stop`** at a command prompt. To make sure it does not start again, delete or rename the `/etc/init.d/sendmail` executable.

To stop `sendmail` on Linux*, type **`/etc/rc.d/init.d/sendmail stop`**. To make sure it does not get started again, delete or rename the `/etc/rc.d/init.c/sendmail` executable.

Messaging Server Shows High Utilization

Problem: The messaging server's utilization never drops below 99%.

Possible Cause: High utilization is not necessarily a bad thing. If the server has work to do, high utilization indicates that the software is making efficient use of the CPU.

When there is little or no messaging traffic, high utilization usually indicates a software loop.

The most common mail loop in NIMS occurs when a hostname or domain name published in DNS resolves to a messaging server but is not added to the SMTP Agent's domain/hostname list.

For example, the domain name "companyx" is published as an A or MX record and it resolves to the current messaging server. When a message is sent to `user@companyx.com`, the SMTP Agent looks up the domain name in DNS and sends the message to the corresponding IP address. Since that IP address is its own, the SMTP Agent actually sends the message to itself, re-entering the message in the queue. However, because the domain name is not in the SMTP Agent's domain list, it does not claim the message. Consequently, the SMTP Agent starts the loop again by resending the message.

Action: To resolve the problem, add all host and domain names that resolve to any server in the messaging system to the SMTP Agent's Domain list. See **"SMTP Agent: Identification" on page 80**.

Looping messages are usually very easy to spot in the queue directory. Copy all files in the spool directory to a temporary directory. Then, look for files that start with the letter D (the data file) and are abnormally large. Open those files in an editor to see if the SMTP Agent has made more than a few entries (usually hundreds) in the message header.

Once such a message is found, look for the message's control file envelope (a file with the same name, but that starts with the letter C). This file contains the addresses to which the SMTP Agent is trying to deliver the message.

Distributed Messaging System Is Not Functioning

Problem: You have a single NMAP Agent with other POP, SMTP, WebMail, Alias, and Address Book Agents distributed over several other messaging servers. The messaging system is not functioning in distributed mode. Users cannot send or receive messages; the Alias Agent cannot generate aliases, and the Address Book Agent cannot locate users within the messaging system.

Action: If you are running your messaging system in distributed mode, every agent must be a trusted host of the NMAP Agent in order to access the message store and message queues. If you have multiple NMAP Agents, the NMAP agents must be trusted hosts of each other. [“NMAP Agent: Trusted Hosts” on page 77.](#)

Standalone Messaging System Can Send Messages to the WAN but Cannot Receive Them

Problem: You are operating in a WAN environment with multiple standalone messaging servers and at least one central distributed messaging server. You have configured the Forward Local Undeliverable Messages option so the standalone messaging servers can send mail through a distributed messaging server to the rest of the messaging system; however, the standalone servers cannot receive mail from the rest of the messaging system.

Action: In order for a standalone messaging server to receive mail from a distributed messaging server, the standalone messaging server must have an alias object in the Internet Services container. See [“Creating an Alias for Each Remote Messaging Server” on page 57.](#)

NIMS System Must Service Users in Multiple NDS Trees

Problem: You want to support multiple NDS trees with a single messaging system.

Action: Use the Forward Local Undeliverable Messages option to send messages between messaging servers in different NDS trees. See “**NMAP Agent: Options**” on page 74.

Administrator Wants to Uninstall NIMS

Problem: The administrator wants to uninstall NIMS.

Action: To uninstall NIMS from a NetWare® server:

- 1** Delete the NIMS NLM programs from the SYS:\SYSTEM directory.
- 2** At the console prompt, type **load nimsext**.
- 3** Enter your admin user name and password.
- 4** Select Remove Schema Extensions > press Enter.

This will remove NIMS objects in Internet Services. NIMS objects located outside the Internet Services container must be manually deleted.

- 5** Press Enter to confirm the removal of NIMS schema extensions.
- 6** Exit the NIMSEXT utility.

- 7** Delete NIMS.DLL and SYSLSNAP.DLL from the PUBLIC:\WIN32\SNAPINS directory.

This will hide the NIMS properties added to standard NDS objects such as the User and Server objects.

Action: To uninstall NIMS from a Solaris server:

- 1** At the command prompt, enter **/opt/NOVLnims/bin/nimsext**.
- 2** Enter your admin user name and password.
- 3** Select Remove Schema Extensions > press Enter.

This will remove NIMS objects in Internet Services. NIMS objects located outside the Internet Services container must be manually deleted.

- 4** Press Enter to confirm the removal of NIMS schema extensions.
- 5** Exit the **nimsext** utility.

- 6** At the command prompt, type **pkgrm NIMS**.
- 7** Delete your message store directories.

Action: To uninstall NIMS from a Linux server:

- 1** At the command prompt, enter **/usr/local/nims/bin/nimsext**.

- 2** Enter your admin user name and password.
- 3** Select Remove Schema Extensions > press Enter.

This will remove NIMS objects in Internet Services. NIMS objects located outside the Internet Services container must be manually deleted.

- 4** Press Enter to confirm the removal of NIMS schema extensions.
- 5** Exit the `nimsext` utility.
- 6** At the command prompt, type **`rpm --erase NIMS`**.
- 7** Delete your message store directories.

D

Setting Up SSL

Internet mail protocols such as POP3, IMAP4, and SMTP are not inherently secure. Organizations concerned with securing client-to-server communications must use SSL. SSL secures client-to-server communications by encrypting the complete communication flow between email clients and mail servers.

To secure communications between NIMS messaging servers and all email clients, NIMS supports SSL on all protocols, including WebMail and WebAdmin.

The following is a listing of the NIMS default SSL port assignments by agent:

- ♦ WebMail—443
- ♦ WebAdmin—444
- ♦ POP—995
- ♦ IMAP—993
- ♦ SMTP—465

NOTE:

To use SSL on your messaging system, you must obtain a server certificate from a Certificate Authority (CA).

The following topics help you set up and use SSL with your NIMS system:

- ♦ [“Certificate Authority” on page 172](#)
- ♦ [“Obtaining a Server Certificate” on page 172](#)

- ♦ “Generating a Certificate Signing Request” on page 173
- ♦ “Using CERTGEN to Generate a CSR” on page 173
- ♦ “Installing the Server Certificate” on page 175
- ♦ “Installing the Root Certificate to a Server” on page 176
- ♦ “Installing the Root Certificate to Email Clients” on page 177

Certificate Authority

A Certificate Authority (CA) is a trusted third party that issues digital certificates to other entities (organizations or individuals) to allow them to prove their identity. In most cases, the CA is an external company that offers digital certificate services. In some instances, however, organizations generate and maintain their own digital certificates using CA servers such as the Novell® Certificate Server .

One company that provides digital certificate services is Thawte* Certification. For more information on Thawte and digital certificate services, visit [Thawte Digital Certificate Services \(http://www.thawte.com/\)](http://www.thawte.com/).

To select a CA, you may want to check your email client to determine which CAs it already supports. If you use one of these providers, you won't need to install root certificates for your CA on all of your email clients.

Obtaining a Server Certificate

The first step in obtaining a server certificate from your CA is to submit a Certificate Signing Request (CSR). When the CA receives your CSR, it goes through a process of verifying your identity. Once it has verified your identity to its satisfaction, the CA digitally signs your CSR. This digitally signed CSR is your server certificate. The CA's signature attests to all other parties that you are who you say you are. Your organization's server certificate must be installed on every messaging server on which you want to use SSL.

Most certificates expire and must be renewed at regular intervals. To maintain SSL functionality, you must keep your certificate current.

Generating a Certificate Signing Request

A CSR is an electronic file that contains information about your organization. The CSR also includes a series of unique variables that are used to distinguish your organization's server certificate. In order to be accepted by a CA, the CSR must conform to Public Key Cryptography Standards (PKCS).

CERTGEN is the NIMS utility used to generate a CSR. (It is also used to install and renew the server certificates you receive from your CA.) This Windows* executable is located in your messaging server's SYS:\SYSTEM directory.

Before You Start

Before launching CERTGEN, you will need to collect the following information:

- ♦ The fully qualified DNS name of your messaging server.
- ♦ The Organization (O) and Organizational Unit (OU) your mail system belongs to. (These should not be confused with Organizations and Organizational Units in NDS®.) If your CA does not assign these values, they are arbitrary.
- ♦ In most cases, you will enter your CSR at the CA server or Web site; however, if you are required to email your CA request, you will need the IP address or host name of a mail relay host (SMTP Agent) so CERTGEN.EXE can mail your request.

Using CERTGEN to Generate a CSR

To generate a CSR:

- 1** From a Windows workstation, run CERTGEN.EXE (located in the SYS:\SYSTEM directory).
- 2** Select the drive that is mapped to the SYS: volume on the server where you want to install the certificate > click Next.
- 3** Select Request a New Certificate > click Next.

IMPORTANT:

4 Complete the information in the requested fields.

You cannot tab between these fields. Use your mouse to click in each field.

If you are using a public CA, this information will be used to notify you when your certificate needs to be renewed.

The person responsible for maintaining the server certificate.

The contact address for the person maintaining the server certificate.

Refers to the fully qualified DNS name of your messaging server.

The organization name assigned by the CA. If the CA does not assign the name, use your own.

The organization unit assigned by the CA. If the CA does not assign this name, use your own.

These items indicate your organization's location. In the Country field, enter your country's 2-digit code.

5 Select a method for delivering the certificate > click Next.

For more information, visit [Novell Certificate Server \(http://www.novell.com/products/certserver/\)](http://www.novell.com/products/certserver/).

- 6** At the final screen, click Finish.

Installing the Server Certificate

Once the CA has verified your identity to its satisfaction, the CA sends you a server certificate. The server certificate is actually your CSR with the addition of the CA's digital signature. This server certificate must be installed on every messaging server on which you wish to use SSL.

The server certificate should be installed on any server running an agent that is accessed by email clients. This would include servers running the POP, IMAP, SMTP, WebMail, and WebAdmin Agents.

To install the server certificate to a messaging server:

- 1** From a Windows workstation, run CERTGEN.EXE (located in the SYS:\SYSTEM directory) > click Next.
- 2** Select the drive that is mapped to the SYS: volume on the server where you want to install the certificate > click Next.
- 3** Select Install a Certificate Received from a CA > click Next.
- 4** In another window, open the server certificate in a text editor such as Notepad.
- 5** Select the entire certificate (including the Begin and End lines) and copy it into the Windows clipboard.
- 6** Once you have copied the certificate of authority to the Windows clipboard, click Next in CERTGEN.
- 7** At the final screen, click Finish.
- 8** Restart the messaging server.

The server certificate has now been installed on the designated messaging server.

Installing the Root Certificate to a Server

After installing your server certificate, you must install the CA's server certificate, otherwise known as a root certificate. The root certificate identifies the CA, thereby validating the CA's signature on the server certificate. Without the root certificate, the messaging server has no way of knowing who the CA is or if its signature is valid. Consequently, it cannot "trust" the server certificate.

IMPORTANT:

To install the CA's root certificate to a messaging server:

- 1** From a Windows workstation, run CERTGEN.EXE.
- 2** Select the drive that is mapped to the SYS: volume on the server where you want to install the root certificate > click Next.
- 3** Select Add/Renew a Trusted Certificate Authority (CA) > click Next.
- 4** Select the location of the root certificate > click Next.

Requires that you open the encoded certificate in another window and copy the entire certificate (including the Begin and End lines) into the Windows clipboard.

Requires that you have the encoded or raw certificate accessible from the current workstation.

- 5** If you selected From Clipboard, the root certificate is automatically copied from the Windows clipboard.

or

If you selected From a File, CERTGEN brings up Windows Explorer. Browse the directory structure to locate the root certificate and click Open.

The accepted file types are PKCS12 Certificates or raw X.509 certificates.

- 6** Enter a name for your root certificate > click Next.
- 7** At the final screen, click Finish.

Installing the Root Certificate to Email Clients

Installing the root certificate to your email clients is necessary only if your email client (or, in the case of WebMail and WebAdmin, your browser) does not recognize your CA.

To determine which CAs are recognized by your client, locate the list of supported CAs in your email client or browser.

- ♦ In Netscape or Netscape Communicator, click Communicator > Security Info > Certificates > Signers.
- ♦ In Internet Explorer or Outlook Express, click Tools > Internet Options > Content > Certificates > Trusted Root Certificate Authorities.
- ♦ For specific email clients, refer to the email client's Help.

If your CA is not supported, ask your CA for instructions on adding its root certificate to your email client or browser.

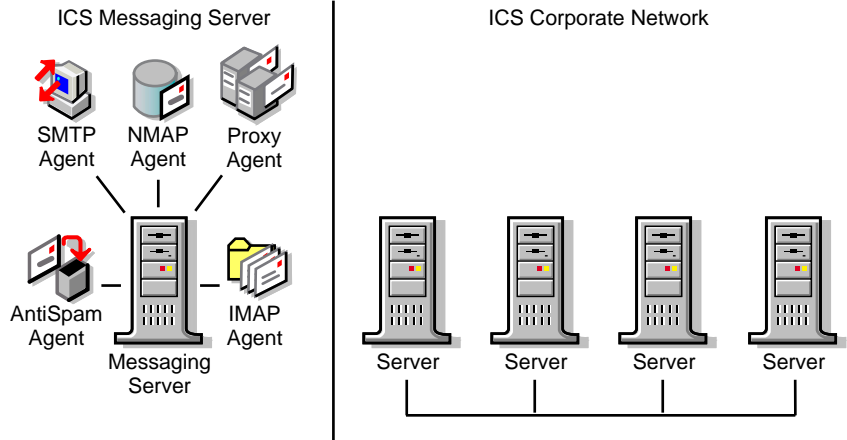
E

Sample NIMS Configurations

- ♦ “Single Server Tree Example” on page 179
- ♦ “Single Messaging Server Example” on page 180
- ♦ “Independent Messaging Server System Example” on page 181
- ♦ “Distributed Messaging Server System Example” on page 182
- ♦ “Hub-and-Spoke Messaging System Example” on page 183

Single Server Tree Example

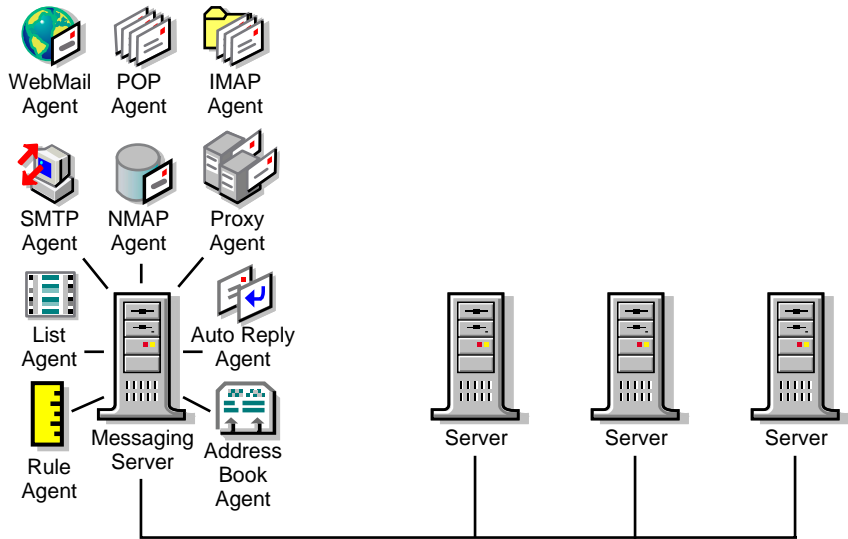
In this example, ICS is an ASP that provides email services to 3,000 small businesses in the Tri-City area through a single server network. Currently, ICS supports approximately 80,000 mail accounts with access to WebMail, POP, IMAP, SMTP, Alias, AutoReply, Proxy, and Rules. The company has an internal LAN; however, to secure the corporate network, ICS has chosen to isolate the messaging system from the rest of the network.



Given the number of users, the services provided, and the fact that the messaging system is isolated from the rest of the network, a single server network configuration is best suited for ICS' needs. A dedicated messaging server is amply equipped to handle projected usage with a single Pentium* III 550 MHz processor, 3 GB of RAM, and 1 TB in disk space.

Single Messaging Server Example

In this example, Vergo Enterprises currently has a single LAN with three servers and 1500 workstations. A messaging system of this size running WebMail, POP, IMAP, Address Book, SMTP, AutoReply, Proxy, List, and Rules can be managed with one additional dedicated messaging server with a Pentium II 300 MHz processor, 512 MB of RAM, and 10 GB in disk space.



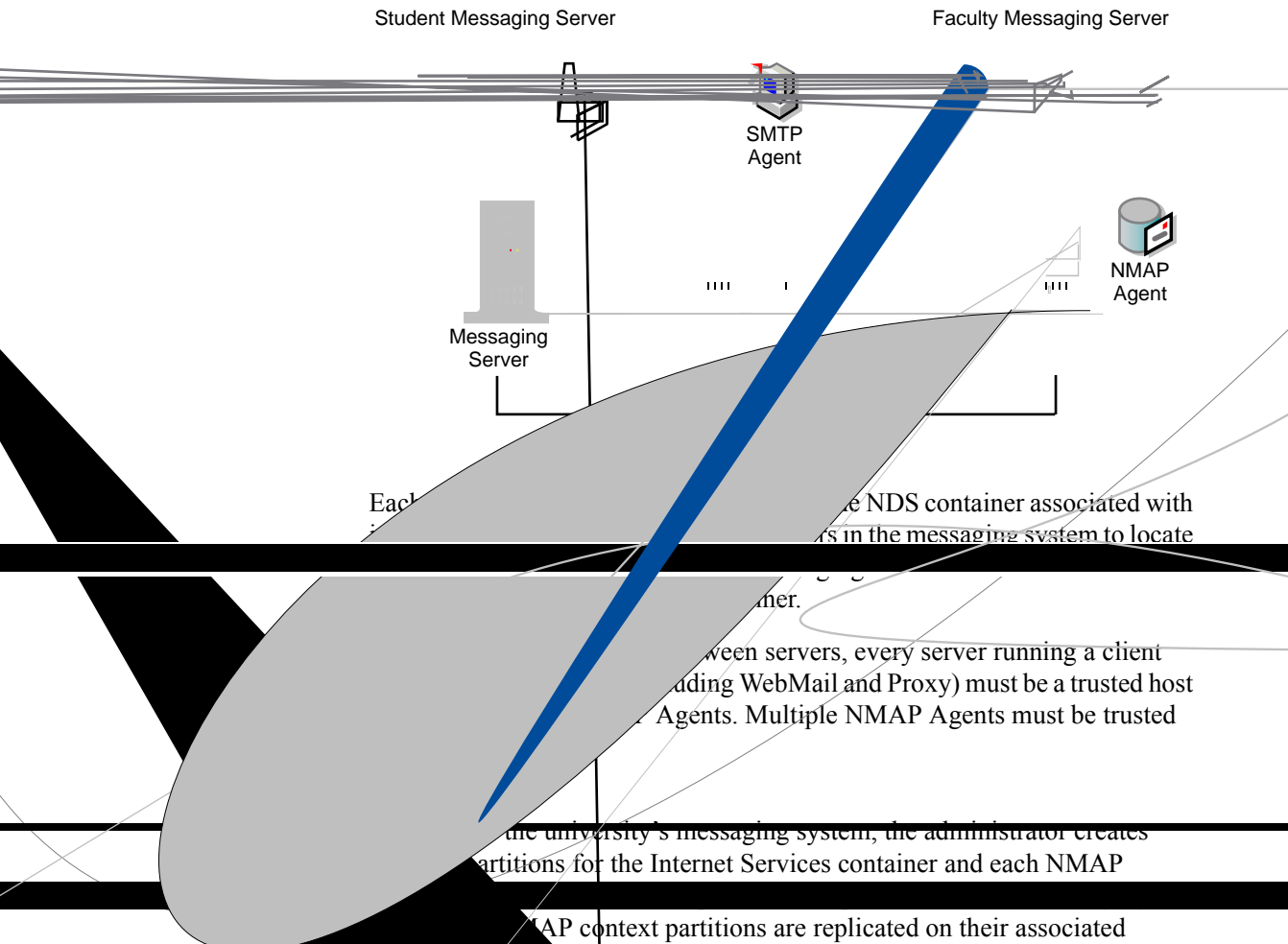
Given that the current network has three servers, the fourth (NIMS) server does not have local access to NDS[®]. To ensure NIMS performance, the administrator partitions the Internet Services container and the NMAP Agent's user contexts and replicates the partitions on the messaging server.

Independent Messaging Server System Example

In this example, StormFront is a large ASP that hosts domains and Web pages for a broad range of corporate accounts. In addition to their domain hosting services, StormFront provides groupware and electronic messaging for their clients.

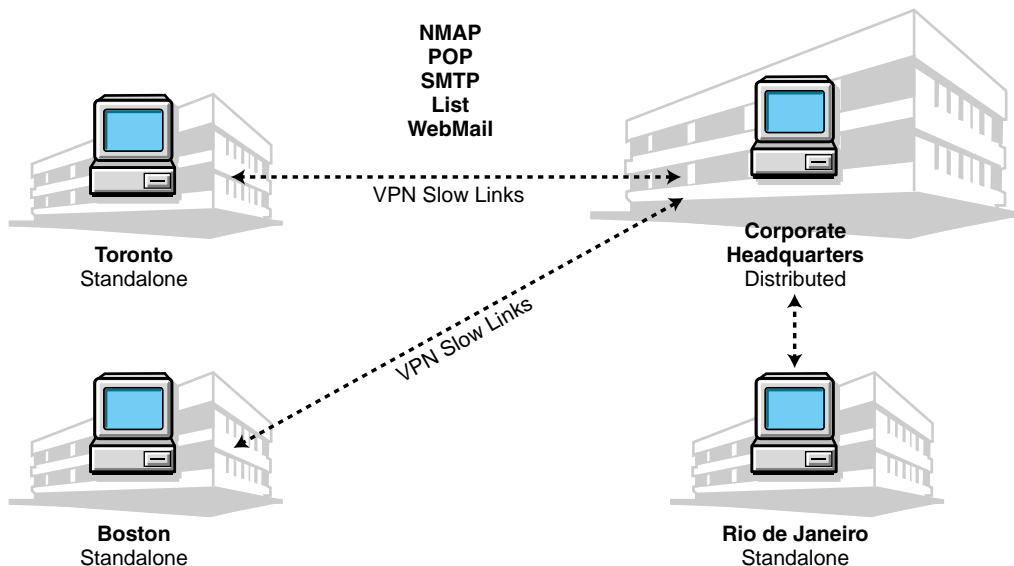
To service their electronic messaging accounts, each of which has a separate domain name, StormFront uses multiple independent messaging servers. For example, two of StormFront's largest customers, FleetFoot and DogBeClean, each have independent messaging servers.

dog(ecl)an.-om



Hub-and-Spoke Messaging System Example

In the example of an international pharmaceutical company. The Research and Development department, New Jersey and is located in Boston, Massachusetts. Due to the large number of its offices, there is a need for a messaging system.



To minimize network traffic across WAN connections while still providing fast, efficient service to all users, a distributed messaging system is located at corporate headquarters in Princeton, while Boston, Toronto, and Rio have remote standalone messaging servers.

Because the servers in Boston, Toronto, and Rio are remote messaging servers, they cannot locate and interact with other servers in the central messaging system. Conversely, the distributed messaging system in Princeton cannot locate or interact with them because they are not represented in the Internet Services container. Consequently, users throughout the messaging system can neither send nor receive messages from users in the remote offices. Integrating the remote and distributed messaging servers requires additional configuration.

To enable users in remote offices to send messages to the central messaging system, the Boston, Toronto, and Rio servers must be configured to forward local undeliverable messages to Princeton's distributed messaging system.

To enable the central messaging system in Princeton to send or forward messages to users in Boston, Toronto, and Rio, the remote messaging servers must be represented by a Alias objects in the Internet Services container.

To optimize the connection between Princeton and the remote servers, Princeton's messaging server is a trusted host of the Boston, Toronto, and Rio servers' NMAP Agents.

To ensure optimal performance in a WAN environment, every messaging server (specifically, the remote servers) must have local access to its associated Messaging Server and User objects.

On remote servers, this is done by grouping the server's Messaging Server and User objects in a single partition and then replicating that partition on its respective messaging server. In order to minimize network traffic, these objects are grouped in a single partition to reduce the total number of partitions that must be replicated over each WAN connection to one.

The distributed messaging server requires local access to Internet Services and its assigned user contexts. Therefore, the administrator partitions and replicates both Internet Services and the server's user contexts. Because the distributed messaging server operates in a fast link environment at the network's hub, replicating multiple partitions on the server does not slow the system's overall performance.

Because the servers in Boston, Toronto, and Rio are remote messaging servers, they cannot share messaging functions with other servers. Consequently, the NMAP, POP, IMAP, Finger, SMTP, AutoReply, WebMail, Connection Manager, AntiSpam, Alias, and Proxy Agents must all run locally on the Boston, Toronto, and Rio servers.

The one exception is the Address Book Agent. Reesis wants a corporate address book. Because the remote servers have access only to their local NDS partitions, they cannot "see" all the users in the network. The only server with access to the entire tree (and therefore, to all the users within the messaging system) is Princeton's messaging server.

Therefore, the Address Book Agent must be installed on the Princeton messaging server. To access the Address Book Agent, users configure the email client to use the Princeton messaging server as an LDAP server. In their email client System or Public address book fields, users enter the host name and LDAP port number of the Princeton server. The Address Book Agent's default LDAP port assignment is 389.

F

Supported Standards

The following is a list of NIMS agents and their supported standards.

RFC	Title	Applies To
-----	-------	------------

