Novell NetMail™

3.5

www.novell.com

NOVELL NETMAIL ADMINISTRATION GUIDE

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell NetMail 3.5 Administration Guide
October 2003

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/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.

NCP is a trademark of Novell, Inc.

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 Services is a trademark of Novell, Inc.

Novell NetMail is a trademark of Novell, Inc.

Novell Nterprise 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.

Preface

Welcome to Novell® NetMail™ 3.5, the premier Internet standards-based messaging system. This *Administration Guide* provides information to design, install, and manage your NetMail messaging system.

Rather than simply presenting a series of step-based instructions, this manual provides the concept behind the procedure. Our goal in this approach is to help you understand how NetMail works so you can configure it to meet the specific needs of your Internet messaging environment.

NOTE: For additional troubleshooting information and available TIDs (Technical Information Documents) from Novell Technical Support, reference NetMail FAQ (http://www.novell.com/coolsolutions/netmail/features/a_nims_faq_nm.html) and search the Novell Knowledgebase for NetMail at NetMail Cool Solutions Home Page (http://www.novell.com/coolsolutions/netmail),

Content Map

To help direct you to those sections that address your particular needs, the following sections provide an overview of each chapter and note its target audience. We have also directed you to specific topics where system function have changed or new features are available.

Chapter 1: NetMail System Overview

Chapter 1 provides a "big picture" view of NetMail and its components, and how it works. It is designed to give you a clear understanding of NetMail architecture and functionality. The "NetMail Components" on page 2 section reviews the functionality of NetMail's agents and objects. The "Message Processing" on page 19 section explains message processing both in terms of its directory infrastructure and the actual process.

Chapter 1 is an ideal starting place if you are new to NetMail. For experienced NetMail administrators, Chapter 1 introduces those components new to NetMail 3.5 and it provides a sound review of message processing.

Chapter 2: Planning Your NetMail System

Chapter 2 reviews the basic NetMail configurations and their respective requirements. It is designed to help you decide which NetMail configuration best suits your organization's needs and how to implement that configuration.

Of particular interest is "Creating and Configuring NetMail Agents" on page 35. It presents basic agent distribution strategies for those who are implementing a distributed messaging system.

Chapter 2 specifically targets administrators who are deploying new Internet messaging systems or expanding existing messaging systems.

Chapter 3: Installing NetMail 3.5

Chapter 3 presents NetMail 3.5 system requirements and prerequisites and then guides you through the installation and initial launch of NetMail 3.5.

This section is for all administrators, whether they are installing NetMail for the first time or upgrading from a previous version.

Chapter 4: Configuration Basics

Chapter 4 introduces NetMail's configuration tools and basic configuration concepts.

This section primarily targets administrators who have little or no experience with NetMail and eDirectory™.

Chapter 5: Setting Up Your Messaging Server and NMAP Agent

Chapter 5 helps to successfully create and configure your system's messaging server and NMAP Agent.

Because the messaging server and NMAP Agent are critical in building a functional messaging system, this section should be reviewed by administrators who are new to NetMail.

Chapter 6: Configuring E-mail Services

Chapter 6 is designed to help you successfully create and configure your messaging system's e-mail services.

New NetMail administrators should review this chapter to plan and deploy their system's e-mail services.

Chapter 7: Using WebAccess and Webmail

Chapter 7 reviews the WebAccess and Webmail client interfaces from a user perspective.

This information is helpful for new users. As an administrator, you can extract this information and distribute it to your users.

Chapter 8: System Administration

Chapter 8 outlines ways you can automate or simplify system administration. This section is designed to help you lower your overall IT costs.

Also included are two user-based topics on self-administration. The topics, "Accessing the Self-Administration Options" on page 199 and "Self-Administration Options" on page 200, contain information that can be directly extracted and distributed to your users.

Chapter 8 is a "must-read" for all system administrators.

Chapter 9: Auditing Your Messaging System

In NetMail 3.5, Novell® Nsure™ Audit replaces Syslog as the messaging system logging service. During install, Novell Nsure Audit is automatically configured to write messaging system events to a translated log file. Chapter 9 provides the basic information you need to manage the auditing

system's primary components as installed with NetMail 3.5. It does not provide full coverage on all the capabilities of the Novell Nsure auditing system. For complete documentation, see the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/index.html)

Because Novell Nsure Audit is new to NetMail 3.5, chapter 9 is a "must read" for all administrators.

Chapter 10: Securing Your System

Chapter 10 reviews specific options that can be implemented to secure client/server communications, protect your system from UBE, and prevent your system from being used to relay UBE. Detailed explanations are provided for implementing SMTP-after-POP.

Chapter 10 is a "must read" for new NetMail administrators and anyone setting up TLS/SSL or SMTP-after-POP.

Chapter 11: Hosting and Feature Management

Chapter 11 specifically targets issues that are common to multi-domain messaging systems; however, single-domain administrators will find topics such as "Domain Sharing" on page 251 and "Managing User Aliases" on page 253 helpful.

Chapter 11 also gives a thorough review of Parent objects and how they can be leveraged to manage feature availability and distribute user account management.

This chapter is of particular interest to administrators in multi-domain environments such as ISPs, ASPs, and multi-domain corporations. The "Leveraging Parent Objects" topic should be reviewed by all administrators.

Chapter 12: Managing Mailing Lists

Chapter 12 provides the information you need to configure and manage mailing lists, including a complete explanation of list server commands.

Chapter 12 should be reviewed by all administrators maintaining a NetMail list server.

Appendix A: Sample NetMail Configurations

Appendix A provides practical examples of the NetMail configurations outlined in Chapter 2 and can be used as a follow-up piece to Chapter 2.

Like Chapter 2, Appendix A targets administrators who are deploying new Internet messaging systems or expanding existing messaging systems.

Appendix B: Message Structure

Appendix B reviews the structure of messages as they come into the messaging system, pass through the message queue, and are stored in the user's mailbox or SCMS directory. This information is particularly helpful when identifying message relaying points and troubleshooting mailbox or SCMS problems.

Appendix B provides useful information for all administrators.

Appendix C: Supported Standards

Appendix C lists all NetMail-supported Internet standards, notes their RFC, and identifies the protocol and the associated NetMail Agent. Also included are basic explanations of the e-mail protocols and security standards.

Because the NetMail 3.5 supports several new or updated standards, Appendix C should be reviewed by all administrators.

Appendix D: Port Assignments

Appendix D lists all NetMail default port assignments. It also indicates the port assignments that are configureable.

Because some of the port assignments have changed, Appendix D is a “must read” for all administrators.

Appendix E: Implementing Administrative Changes

Appendix E outlines how much time it takes to implement changes to any NetMail property.

Appendix E provides useful information for all administrators.

Appendix F: NetMail Commands and Utilities

Appendix F reviews NetMail startup commands for NetWare®, Windows*, and Linux* systems. It also outlines the parameters for various server commands and utilities including MAIL, MAILCON, NMAIL, IMSAUDIT, NIMSEXT, MAIL LOAD, and RMBOX.

Appendix F provides useful information for all administrators.

Appendix G: Optimizing a NetWare Server for NetMail

Appendix G outlines the steps to optimize NetWare servers for NetMail.

Appendix G provides useful information for all administrators using NetWare servers.

Appendix H: NetMail Configuration

Appendix I compiles information presented in earlier sections to provide a centralized “quick-reference” for all configuration information.

Appendix I: Quick Reference Matrix

Appendix J provides a quick reference of commands, file structure, and available utilities for each supported operating system.

Documentation Updates

For the most recent version of the Novell NetMail Administration Guide, see the Novell Documentation Web site (http://www.novell.com/documentation).

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single path name can be written with a backslash for some platforms or a forward slash for other platforms, the path name is presented with a backslash. Users of platforms that require a forward slash, such as UNIX*, should use forward slashes as required by your software.

1 NetMail System Overview

This section provides a “big picture” view of Novell® NetMail™ and its components, and how it works. It also provides general information on Novell Nsure Audit, the auditing system that has been integrated in NetMail 3.5. The following information is designed to give you a clear understanding of NetMail architecture and functionality so you can better design, configure, and maintain your NetMail system.

Section topics include

- “NetMail Components” on page 2
  - “Internet Services” on page 2
  - “Messaging Server” on page 2
  - “Parent Objects” on page 5
  - “Templates” on page 6
  - “Mailing Lists” on page 7
  - “NetMail Agents” on page 8
- “Novell Nsure Audit Components” on page 13
  - “Logging Services” on page 14
  - “Logging Server” on page 14
  - “Application Objects” on page 15
  - “Channel Objects” on page 15
  - “Notification Objects” on page 16
- “NetMail Attributes in Existing Directory Objects” on page 18
  - “NCP Server Objects” on page 18
  - “Container Objects” on page 18
  - “User Objects” on page 18
- “Message Processing” on page 19
  - “Message Store” on page 19
  - “Single Copy Message Store” on page 20
  - “Message Queue” on page 21
  - “Message Processing in the Message Queue” on page 21

NetMail Components

NetMail has a highly modular architecture that provides tremendous flexibility without compromising system integrity. Product functions are strategically divided among several different components so you only need to install the components required for your system. Based on usage and system resources, you can locate those components on a single server or distribute them across multiple servers.

A general description of each component is provided in the following sections.

Internet Services

Description: Internet Services icon

During your initial NetMail installation, the installation program extends the Novell eDirectory™ schema and creates the Internet Services container object at the root of your Directory tree. Because it is part of NetMail, the Internet Services container differs from other eDirectory Container objects. Only one Internet Services container can exist per tree and, as the messaging system container, it only contains NetMail component objects.

If the Internet Services container is deleted, it can only be recreated by running NIMSEXT. For more information on the NIMSEXT utility, see "NIMSEXT" on page 332.

Messaging Server

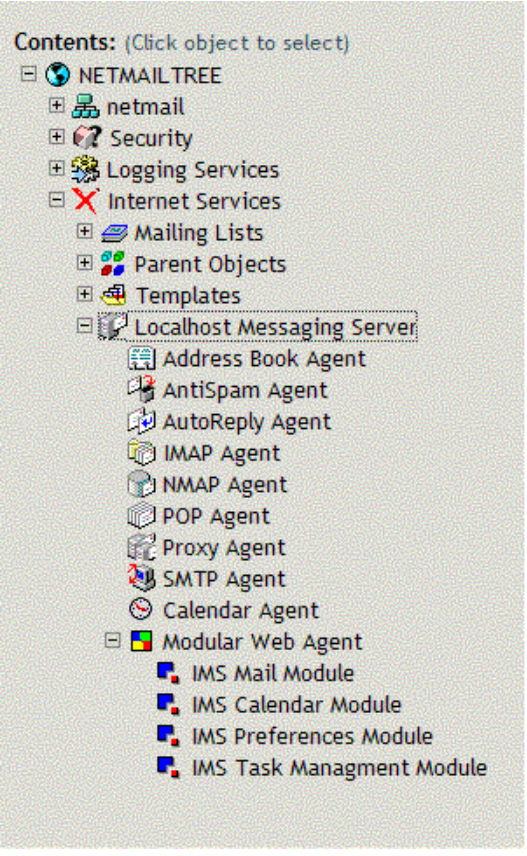
Description: Messaging Server icon

A messaging server is any server on the network that hosts one or more NetMail agents. In the eDirectory tree, the Messaging Server object represents the physical server where the NetMail software is installed.

The Messaging Server object is represented as a container with server attributes; it contains one or more agent objects and it defines the messaging server properties. For a complete explanation of each agent's configuration options, see Appendix H, "NetMail Configuration," on page 343.

Because the Messaging Server object is NetMail specific, it does not replace the NCP Server object. Instead, each Messaging Server object is associated with an NCP Server object in the tree.

Description: The eDirectory tree



Because of NetMail's building block architecture, you can implement your entire messaging system on a single server or distribute NetMail services across multiple messaging servers. In environments with multiple messaging servers, you can configure the servers to work together as a single, integrated messaging system (distributed environment), or let them operate as independent subsystems (standalone environment).

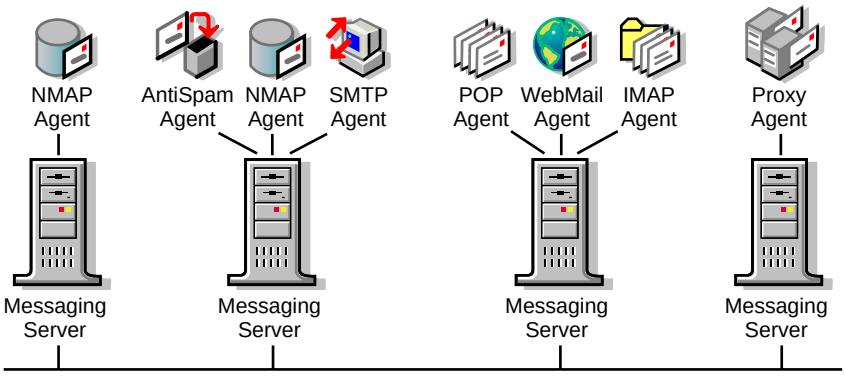
NOTE: For help in determining if a standalone or distributed messaging server would best suit your messaging environment, see "Selecting Your NetMail System Configuration" on page 28. For specific information on creating and configuring the messaging server, see "Messaging Server" on page 59.

Distributed Messaging Servers

In a *distributed messaging system*, multiple messaging servers work together as a single, integrated system. Distributed messaging servers are able to work together because they look for other Messaging Server objects in the Internet Services container. If a Messaging Server object or an alias of that object exists in Internet Services, other distributed messaging servers can find and interact with it. By default, messaging servers are created in distributed mode.

Distributed messaging servers are most often used in larger messaging systems such as ISP, ASP, and multi-LAN environments. Because of message traffic volume, performance requirements, or the local distribution of the network, these organizations typically require multiple messaging servers to provide the load balancing, fault tolerance, and speed needed to service their customers.

Description: Distributed messaging servers



The following examples illustrate ways to use distributed messaging servers to achieve specific system goals:

- To insulate your messaging system from denial-of-service attacks, you can run the SMTP Agent with an NMAP Agent on a dedicated server. If you assign the NMAP Agent a context without any users, its sole function is to handle all incoming SMTP messages. Therefore, in the event of a spam attack, no users are impacted and the remaining NMAP Agents are free to continue processing and delivering messages.
- To optimize e-mail client performance on systems with a high volume of client usage, run the POP, IMAP, and Modular Web Agents on a dedicated, high-performance, e-mail server.
- In environments with heavy proxy usage, create a dedicated Proxy server and configure the Proxy Agent to query its user accounts every hour.

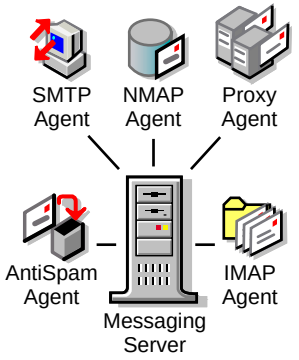
For specific agent distribution strategies, see “Creating and Configuring NetMail Agents” on page 35.

Standalone Messaging Servers

A *standalone messaging server* does not interact with other messaging servers. Instead, it acts as an independent messaging system, exclusively providing all NetMail services to the users within its assigned contexts.

By default, messaging servers are created in distributed mode. To configure a standalone messaging server, you must mark the Distributed Processing Disabled option in the messaging server’s Properties menu. This prevents the messaging server from looking for other Messaging Server objects in the Internet Services container.

Description: Standalone message server



The two most common situations to use standalone messaging servers are

- Messaging systems where a single messaging server is sufficient to handle all message traffic. Although a single server messaging system is very simple in its configuration, such a system is capable of providing efficient messaging services for 250,000-300,00 users (What are the new benchmarks?) and processing over 1,000,000 messages per day. For information on deploying single server messaging systems, see “Single Messaging Server LAN” on page 30.
- WAN environments with slow links. Standalone messaging servers are a means of providing NetMail service to users in remote offices without overextending your bandwidth and reducing the performance of the rest of your messaging system. For more information on configuring NetMail in WAN environments, see “Multiple Messaging Server WAN” on page 288.

Parent Objects

Description: Parent object icon

Parent objects enable administrators to collectively manage agent services and user settings for specific sets of users. This functionality enables the administrator to subdivide a single messaging system into configuration subunits. For example, by creating separate Parent objects for each domain, administrators can manage every domain as if it were a separate messaging system.

The Parent object is a collective management tool that offers other significant advantages. The configuration options in the Parent object allow administrators to selectively grant access to messaging services. This means that although an agent is running on the messaging server, not everyone can access the agent’s services. Instead, the administrator can enable or disable different agent services for each Parent object. For example, in an ISP environment, the system administrator could use Parent objects to give one Hosting Domain access to POP and another access to IMAP. This allows the ISP to bill for individual services. (For more information on using Parent objects to manage messaging services, see “Feature Management” on page 261.)

You can also use Parent objects to distribute administrative tasks. You can give selected users rights to create, delete, modify, or import user accounts in specific Internet domains. For example, in a corporate environment, the system administrator could use Parent objects to give administrative assistants rights to create their department’s user accounts. Because all administrative functions are performed in WebAccess, the operations are familiar, intuitive, and user-friendly. Moreover, users do not need to know anything about eDirectory. (For further information, see “Task-Oriented Management” on page 262.)

Agents running on both distributed and standalone messaging servers dynamically look up the user’s Parent object in the tree to determine what rights the user has to the service.

For more information on creating and configuring Parent objects, see “Leveraging Parent Objects” on page 260.

Parent Container

Description: Parent Container icon

The Parent container is created in Internet Services during installation. This container is the centralized location for Parent objects. NetMail agents reference the Parent container when looking up user configuration information.

IMPORTANT: Every Parent object must be represented in the Parent container for NetMail Agents to find it. If a Parent object is created elsewhere in the tree, it must be represented by an Alias object in the Parent container. (You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Parent container.)

If the Parent container is deleted, it can only be recreated by re-running NIMSEXT. For more information on the NIMSEXT utility, see "NIMSEXT" on page 332.

Templates

Description: Template icon

The Modular Web Agent provides two template-based, mail client interfaces: WebAccess (Webacc.ctp) and Webmail (WebMail.ctp).

The WebAccess interface provides standard mail client functionality, calendaring, scheduling, tasks, notes, and busy search along with user self-administration features like changing passwords and configuring vacation messages. Administrators can also use the WebAccess interface to give selected users access to administrative functions such as adding, modifying, and deleting user accounts.

Webmail is patterned after the NIMS 2.5 mail client interface. Like WebAccess, it provides standard mail client functionality, calendaring, scheduling, tasks, notes, and user self-administration tasks like changing passwords and configuring vacation messages. However, WebMail does not provide busy search or administrative functions like adding, modifying, and deleting user accounts.

Webacc.ctp and WebMail.ctp each contain everything needed to present their respective client interfaces; images, web pages, localized text, etc. are all compiled in these two template files. Consequently, NetMail no longer needs to install multiple mail client directories. When the Modular Web Agent initializes on the messaging server, it simply loads the template files into memory.

The WebAccess and WebMail objects must be created in the tree before they can be loaded on the messaging server or selected in the Modular Web Agent, Parent, and User objects.

For more information on creating and configuring Template objects, see "Calendar Agent" on page 99.

Templates Container

Description: Templates container icon

The Templates container is created in Internet Services during installation. This container is the centralized location for template objects. The Modular Web Agent references the Templates container when scanning for available templates.

IMPORTANT: Every Template object must be represented in the Templates container for the Modular Web Agent to find it. If a Template object is created elsewhere in the tree, it must be represented by an Alias object in the Templates container. (You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Template container.)

If the Templates container is deleted, it can only be recreated by re-running NIMSEXT. For more information on the NIMSEXT utility, see "NIMSEXT" on page 332.

Mailing Lists

The NetMail List Agent allows administrators to create and maintain mailing lists. Mailing lists are essentially public communication forums. They are used to broadcast information via e-mail. NetMail provides two types of mailing lists: list server Mailing Lists and NDS® Mailing Lists.

For more information on creating and configuring list objects, see Chapter 12, "Managing Mailing Lists," on page 269.

Mailing Lists

Description: Mailing List icon

A list server mailing list is a compilation of user e-mail addresses. When a message is sent to the mailing list, the message is automatically forwarded to every user in the mailing list.

Typically, users subscribe to list server mailing lists. To subscribe, users send a message to the list server's e-mail address with the word "subscribe" in the body of the message.

List User Objects

Description: List User Object icon

List User objects represent the members of a Mailing List. When users subscribe to a mailing list, a List User is added to the respective Mailing List object. Administrators can also add mailing list members by creating List User objects within the Mailing List object.

NDS Mailing Lists

Description: NDS Mailing Lists icon

NDS mailing lists allow you to broadcast messages to eDirectory users. Unlike list server mailing lists, NDS mailing lists are comprised of eDirectory objects rather than user e-mail addresses. Selected eDirectory objects can include Container objects, Groups, organizational roles, aliases, and individual User objects.

NOTE: If a Container object is selected, messages are forwarded to the users within the designated Container object.

Mailing Lists Container

Description: Mailing Lists Container icon

The Mailing Lists container is created in Internet Services during installation. This container holds all of the messaging system's available Mailing List objects. The List Agent references the Mailing Lists container when scanning the message queue for messages addressed to mailing lists.

IMPORTANT: Every Mailing List object must be represented in the Mailing Lists container for the List Agent to find it. If a Mailing List object is created elsewhere in the tree, it must be represented by an Alias object in the Mailing Lists container. (You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Mailing Lists container.)

If the Mailing Lists container is deleted, it can only be recreated by re-running NIMSEXT. For more information on the NIMSEXT utility, see "NIMSEXT" on page 332.

NetMail Agents

NetMail agents are a series of executables that perform specific product functions. These agents have plug-and-play versatility; that is, they can be combined in a variety of configurations and still maintain the functionality of a single, integrated messaging system. This building block architecture allows you to easily distribute NetMail across multiple servers. Depending on agent usage and system resources, each agent can run by itself or in conjunction with other agents on a messaging server.

The following table lists all the NetMail agents and summarizes their contributions to your NetMail system. For a complete explanation of each agent's configuration options, see Appendix H, "NetMail Configuration," on page 343.

Table 1 Overview of NetMail Agents, Icons, and Functions

Agent	Icon	Agent Function
Address Book Agent		The Address Book Agent provides read-only LDAP3 access to eDirectory. Using this agent, any LDAP-compliant application (such as e-mail or address book clients) can access address book information from eDirectory. Information returned about each user depends on the user's privacy level. **NOTE:** Do not confuse the Address Book Agent with the Modular Web Agent's address book feature. The Modular Web Agent address book is a user feature that can look up information in virtually any LDAP-compliant database. The Address Book Agent enables address book clients (such as the Modular Web Agent address book) to query eDirectory for address book information.

Agent	Icon	Agent Function
Alias Agent		The Alias Agent enables your NetMail system to recognize user aliases. You can also use the Alias Agent to automatically populate the User object's Internet E-mail Address property. You can define aliases manually or automatically in the Alias Agent. The automatic aliasing feature pulls information directly from eDirectory to generate aliases for eDirectory User objects. You can automatically generate aliases in the following formats: ◆ Firstname_Lastname@Domain (Steve_Johnston@novell.com) ◆ First Letter+Lastnam@Domain (Sjohnsto@novell.com) **NOTE:** This alias option is limited to eight characters. ◆ Firstname.Lastname@Domain(Steve.Johnston@novell.com) ◆ Full.M.Name@Domain (Steve.W.Johnston@novell.com) ◆ Full_M_Name@Domain (Steve_W_Johnston@novell.com) Manually defined aliases can correspond to any Internet mail address such as webmaster@company.com. The aliases created via the Alias Agent are not defined as Alias objects in eDirectory; rather, they are maintained by the Alias Agent and are specific to the NetMail messaging system. Existing Alias objects are recognized by NetMail, but they function independently of the Alias Agent. Messages addressed to Alias objects are automatically delivered to the associated user's mailbox by the NMAP Agent.
AntiSpam Agent		The AntiSpam Agent automatically allows the Postmaster or NetMail administrator to build a blackout list of undesirable e-mail domains and addresses. Messages sent from domains and e-mail addresses contained in the blackout list are not accepted by your NetMail system.
AntiVirus Agent		The NetMail AntiVirus Agent integrates with McAfee* NetShield*, Command* Antivirus, Computer Associates* InnoculateIT*, and Symantec* CarrierScan* virus engines to provide virus scanning on messages handled by NetMail. If a message contains a virus, the AntiVirus Agent immediately deletes it from the message queue. You can configure the agent to return the message to the sender with a notice indicating what virus the message contained. It can also send a virus alert to the message recipients indicating who tried to send the message and what virus the message contained. Within the messaging system, you can enable virus scanning for all users or limit it to a group of users. Limiting virus scanning to specific users is most applicable to ISP environments where users subscribe to this service. Virus scanning is enabled at the Parent or User objects. **IMPORTANT:** You must install one of these vendors' products before you can use NetMail's AntiVirus Agent.

Agent	Icon	Agent Function
AutoReply Agent		The AutoReply Agent allows users create custom messages that are automatically sent in response to incoming mail. For example, when users go on vacation, they can create a message that lets others know they are unavailable. The AutoReply Agent also enables users to forward their messages to another e-mail address. Users can specify if they want to retain a copy of the message in their NetMail mailbox or simply redirect the message to the designated address. In addition to forwarding messages to another e-mail address, the AutoReply Agent can forward SMS messages to cellular phones and pages. Although it does not configure SMS messages, the AutoReply Agent can recognize a message's format and forward it to the user's designated cellular phone or pager number. The AutoReply Agent is not e-mail client specific. Although users must configure mail forwarding and autoreply messages in the Modular Web client, the agent functions independently of any e-mail client. This is because users' forward and autoreply information is stored in their User objects. Therefore, NetMail can handle forwarding and autoreply messages for users of POP3, IMAP4, and Modular Web clients.
Calendar Agent		The Calendar Agent provides automatic status-tracking information for scheduled appointments, tasks, and notes. When a user schedules a calendar event, the Calendar Agent processes all Accept and Decline responses and automatically updates the event's status information in the event organizer's calendar. Only the user who schedules the event can view who has accepted or declined a calendar event. Attendees only see their own status; every other attendee is viewed as pending. This design avoids the spikes in network traffic that would occur if every attendee updated every other attendee's status. If you choose not to run the Calendar Agent, users receive iCal status messages in their Inboxes. Because the status information is in iCal format, the event organizer might not be able to discern whether a recipient has accepted or declined the appointment. iCal mail clients, such as Microsoft Outlook* XP, also provide automatic status tracking for scheduled appointments. If you are exclusively using an iCal compliant mail client, you can choose to either have NetMail manage status tracking via the Calendar Agent or to have the mail client manage status tracking. If you are using the Modular Web client, you must run the Calendar Agent to provide automatic status tracking for scheduled appointments.
Connection Manager		The Connection Manager Agent keeps track of authenticated users. When a user logs in via POP3 or IMAP4, the POP or IMAP Agent gets the client's IP address and sends it to the Connection Manager Agent. Connection Manager then keeps track of the IP address for a designated time period (the default is 15 minutes). Any agent can query Connection Manager for authenticated IP addresses. In NetMail, this service is utilized by the SMTP Agent for SMTP-after-POP. SMTP-after-POP is a UBE Protection feature that prevents unauthorized users from relaying mail through your messaging system. See "Preventing Others From using Your System to Relay UBE" on page 238 for more information. The Connection Manager Agent listens to other agents on UDP port 689. Ensure it is always protected by a firewall.
Finger Agent		The Finger Agent allows NIMS users to provide customized responses to finger requests from other users. This agent is provided only for backward compatibility and is no longer supported by Novell.

Agent	Icon	Agent Function
IMAP Agent		The IMAP Agent enables IMAP4 clients to download mail from the messaging system. In addition to the basic NetMail memory requirements, the IMAP Agent requires approximately 300 KB per expected simultaneous connection to your NetMail system. For users to access their mailboxes, your messaging system must include at least one POP, IMAP, or Modular Web Agent.
List Server Agent		The List Server Agent enables your NetMail system to function as a list server for two-way, fully interactive discussions to one-way lists that deliver announcements, newsletters, and advertising. The list server works in conjunction with the NDS Mailing List and Mailing List objects. NDS-based mailing lists are built from Container, Group, Role, or User objects while general mailing lists are Internet-based and require the full e-mail address of each subscriber. When you send messages to a mailing list, undeliverable status information is not returned if one of the messages is rejected. For complete information on creating and managing mailing lists, see Chapter 12, “Managing Mailing Lists,” on page 269.
Modular Web Agent		The Modular Web Agent provides the template interfaces for the NetMail mail client. There are two available templates: WebAccess and Webmail. Using either template, users can send and receive mail, manage folders, and set mail preferences from any standard Internet browser. The Modular Web Agent also includes several modules that enable various client functions. ◆ Mail Module: Provides mail and address book functions. ◆ Calendar Module: Enables the WebAccess and WebMail calendar features, including appointments, tasks, and notes. ◆ Preferences Module: Allows users to change their passwords. ◆ Task-Oriented Management Module: Enables the administrator to delegate administrative functions such as creating, modifying, or deleting users. In addition to the basic NetMail memory requirements, the Modular Web Agent requires approximately 300 KB per expected simultaneous connection to your NetMail system. For users to access their mailboxes, your messaging system must include at least one POP, IMAP, or Modular Web Agent.

Agent	Icon	Agent Function
NMAP Agent		The NMAP Agent is responsible for managing message processing and delivery. It coordinates everything that happens from the time a message enters the message queue to when it is delivered to the user's mailbox or passed off for delivery via the Internet. It is the only agent that has direct access to the message store. Consequently, every messaging system requires at least one NMAP Agent and every user within the messaging system must be included in one of the NMAP Agent's contexts. The NMAP Agent's three primary functions are ◆ **Managing the message store**: By default, the NMAP Agent creates a mailbox directory for every User object within its assigned contexts. Because NMAP is the only agent with physical access to the message store, the message store directories are always created on servers running the NMAP Agent. For an explanation of the message store directory structure, see "Message Store Directory Structure" on page 19. ◆ **Managing the message queue**: The NMAP Agent coordinates all message processing in the message queue. Although a single NMAP Agent manages each message queue, message processing is very efficient. NMAP is multi-threaded, and therefore can handle multiple messages simultaneously. The Mail Load utility monitors and regulates the NMAP Agent's thread usage to maintain optimal efficiency. At normal operation, the NMAP Agent processes 30-40 queued messages per second. For a detailed explanation of how NMAP processes messages in the message queue, see "Message Processing in the Message Queue" on page 21. For further information on the Mail Load utility, see "MAIL LOAD" on page 332. ◆ **Providing IP access to the message store and message queue**: All agents needing IP access to the message store or message queue interact with the NMAP Agent using the Network Messaging Application Protocol at port 689. Using this standardized protocol, you can integrate third-party applications with NetMail to provide additional functions such as virus checking, content filters, fax, and voicemail.
POP Agent		The POP Agent enables POP3 mail clients to download mail from the messaging system. In addition to the basic NetMail memory requirements, the POP Agent requires approximately 200 KB per expected simultaneous connection to your NetMail system. For users to access their mailboxes, your messaging system must include at least one POP, IMAP, or Modular Web Agent.
Proxy Agent		The Proxy Agent allows users to manage several e-mail accounts from a central mailbox. Users can retrieve messages from up to three POP3 or IMAP4 e-mail accounts on other messaging systems. All messages retrieved from these accounts are stored in the user's NetMail mailbox as if it were the original destination. **NOTE:** The Proxy Agent cannot retrieve messages from mail systems that do not provide POP3 or IMAP4 access to their mailboxes. Additionally, some e-mail providers allow access to your mailbox only if you log in within a specified IP address range that belongs to the service. These providers assign an IP address upon login. In these cases, Proxy does not work even if it is a POP3 or IMAP e-mail service. Depending on the user settings, you can leave a copy of retrieved messages in the original mailbox or delete the messages from the host server. All proxy information is stored in the User object.

Agent	Icon	Agent Function
Rule Agent		The Rule Agent executes rules defined in the Modular Web client. The Rule Agent is not e-mail client specific. Although users must configure rules in the Modular Web client, the agent functions independently of any e-mail client because users' rules are stored in their User object. Therefore, NetMail executes the configured rules whether the users open their messages in a POP3, IMAP4, or Modular Web client.
SMTP Agent		The SMTP Agent is the gateway between the Internet and your messaging system. Its primary function is to transfer messages to and from the Internet. For users to send local messages from POP or IMAP clients or to send messages over the Internet, you must run at least one SMTP Agent on the messaging server. Because the SMTP Agent is the point of entry for all messages received over the Internet, it controls the domains that the messaging system recognizes. Any domain that resolves to the SMTP server's IP address, you must include in the SMTP Agent's domain list or messages are bounced back to their senders. The SMTP Agent also provides most of NetMail's UBE protection features. Options like reverse DNS lookups, Realtime Blackhole List (RBL*) lookups, and host blocking by IP address protect your system from incoming SPAM, while features like ESMTP authentication, SMTP-after-POP, and restrictions on remote sending by IP address protect your system from spammers using your system to relay SPAM. Additional SMTP Agent options include the following: ◆ A message size limit for inbound and outbound Internet messages. ◆ Controls on standard SMTP commands that pose security risks or facilitate connections with offices that have intermittent Internet connections. ◆ A Mail Relay Host definition that allows you to funnel all remote messages through a single SMTP server rather than having every SMTP Agent individually access the Internet.
WebAdmin		WebAdmin is a browser-based, platform-independent, system management tool. WebAdmin is not represented by an Agent object in eDirectory. Instead, the agent is manually launched at the server. Administrators access WebAdmin through a browser by typing the URL or host name of the messaging server with WebAdmin's port assignment. For example: http://127.5.4.1:89 https://127.5.4.1:449 **NOTE:** By default, WebAdmin uses port 89 for HTTP and port 449 for HTTPS connections. On Novell® Nterprise™ Linux Services, WebAdmin uses port 8018 for HTTP and port 8020 for HTTPS connections. For more information on WebAdmin, see "WebAdmin" on page 51.

Novell Nsure Audit Components

In NetMail 3.5, Novell® Nsure™ Audit replaces Syslog as the messaging system logging service. Novell Nsure Audit is a centralized, cross-platform auditing service that collects event data from the messaging system and writes the data to a single, non-repudiable data store. It is also capable of capturing specific types of events (based on criteria you define) and writing those events to secondary data stores or providing event notification through SMTP or SNMP channels.

Like NetMail, Novell Nsure Audit has a highly modular architecture. Product functions are strategically divided among several different components to protect data integrity, optimize system

performance, and provide maximum flexibility. Depending on usage and system resources, these components can be located on a single server or distributed across multiple servers.

Novell Nsure Audit extends the eDirectory schema to include the following objects:

- Logging Services
- Logging Server
- Application Objects
- Channel Objects
- Notification Objects

Nsure Audit uses these objects to store and look up system configuration parameters.

The following sections provide further information on each configuration object. For complete documentation on Novell Nsure Audit, see the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/index.html)

Logging Services

During your initial installation, Nsure Audit extends the eDirectory schema and creates the Logging Services container at the root of your directory tree. Because it is part of Nsure Audit, there can only be one Logging Services container per tree and, as the logging system container, it only contains Nsure Audit component objects.

Locating all logging system components in the Logging Services container is ideal for organizations that need a simple, easy-to-manage logging system. It also suits organizations that are implementing Nsure Audit as an auditing solution and, for security reasons, want to centrally manage their system. To facilitate distributed administration, however, Nsure Audit components can also be created and managed outside the Logging Services container.

If the Logging Services container is deleted, it can only be recreated by re-running AuditEXT. For more information, see page xxNIMSEXT or AUDITEXTxx.

Logging Server

The Secure Logging Server, the server component in the Nsure auditing system, manages the flow of information to and from the Nsure auditing system. It receives incoming events and requests from the Platform Agents; logs information to the data store; monitors designated events; and provides filtering and notification services.

In eDirectory, the Secure Logging Server is represented by the Logging Server object. The Logging Server object is specific to Nsure Audit and does not replace the NCP Server object. Instead, each Logging Server object is associated with an NCP Server object.

The Logging Server object is represented in eDirectory as a container with server attributes; it can contain Nsure Audit objects and it stores all the properties and attributes for the Secure Logging Server. For information on configuring the Logging Server object, see “Configuring the Secure Logging Server” on page 218.

Application Objects

Application objects are associated with applications that log to or request information from Nsure Audit. These objects store the information required by the logging server to authenticate logging applications.

During installation, NetMail creates its own Application object. Likewise, Novell Nsure Audit creates Application objects for itself (the Naudit Instrumentation), the eDirectory Instrumentation, and the NetWare Instrumentation.

NOTE: The Naudit Instrumentation allows Nsure Audit to audit its own events such as creating Channel or Notification objects. The eDirectory Instrumentation manages logging of eDirectory events and the NetWare Instrumentation provides logging for NetWare and file system events. For information on auditing eDirectory and Nsure Audit events, see "Logging eDirectory, NetWare, and File System Events" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/all8rpn.html#all8rpn).

NOTE: xxThe NetWare Instrumentation is only installed on NetWare versions.

For additional information on Application objects, see "Managing Applications that Log to Nsure Audit" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al0lejc.html#al0lejc).

Application Containers

The NetMail, Naudit, eDirectory and NetWare Application objects are created in the Application container under Logging Services during installation.

Application containers provide a reference point through which the logging server can locate Application objects. At startup, the logging server scans its list of Application containers and loads the included Application object configurations in memory where it can quickly access the information when authenticating applications. For information on configuring the Application Container property on the logging server, see "Configuring the Secure Logging Server" on page 218.

IMPORTANT: The logging server only scans its list of Application containers at startup. Therefore, if you modify an Application object, you must restart the logging server. For information on restarting the logging server, see xx"Secure Logging Server Startup Commands" on page 320.

The Application container under Logging Services is automatically created during installation; however, additional Application containers can be created anywhere in the tree.

Channel Objects

Channel objects store the information the logging server needs to log events or provide event notification through a particular channel. For example, to e-mail events, the logging server uses the SMTP channel; therefore, the SMTP Channel object stores the information the logging server needs to use the SMTP channel like the address of the SMTP server; a username and password; and the recipient, sender, subject, and body of the log message.

Novell Nsure Audit currently supports the following channels:

 CVR

 Oracle (not available on NetWare)

 File

 SMTP

 Java

 SNMP

 MySQL

 Syslog

IMPORTANT: The NetMail™ 3.5 product license authorizes you to use the Nsure Audit program's SMTP, File, and MySQL channels. If you configure and enable the CVR, Java, Oracle, SNMP or Syslog channels, Novell Nsure Audit broadcasts licensing notices every 10 minutes to all your configured channels. (You do not receive notices for an unlicensed channel that is configured, but disabled.) The licensing notice indicates that you should acquire a license when you are done evaluating the additional channels.

For information on the File channel, see "Configuring the File Channel" on page 221. For information on the SMTP and MySQL channels, see "Configuring Other System Channels" on page 222. For information on all supported channels, see "Configuring System Channels" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al6t4sd.html).

Channel Containers

The logging server only looks for Channel objects in Channel containers; therefore, Channel objects can only be created within Channel containers.

Channel containers provide a reference point through which the logging server can locate Channel objects. At startup, the logging server scans its list of Channel containers and loads the included Channel object configurations and their drivers. The drivers and Channel object configurations are then available to provide event notification and to log events. Note that the logging server only loads those drivers that have Channel objects in supported Channel containers. For information on configuring the Channel Container property on the logging server, see "Configuring the Secure Logging Server" on page 218.

IMPORTANT: The logging server only scans its list of Channel containers at startup. Therefore, if you create or modify a Channel object, you must restart the logging server. For information on restarting the logging server, see "Secure Logging Server Startup Commands" on page 320.

The Channel container under Logging Services is automatically created during installation; however, Channel containers can be created anywhere in the tree.

Notification Objects

Nsure Audit provides two kinds of event notification:

- Filtered Notification
- Heartbeat Notification

Filtered notification tells you when a specific event has occurred; heartbeat notification tells you when an event has not occurred. The following sections discuss the objects associated with each notification.

Notification Filter Objects

Notification Filter objects store the criteria the logging server uses to filter system events. They also designate which Channel objects the logging server uses to provide event notification.

When you define a Notification Filter, you specify a value for a given event field. To narrow the results, you can define values for multiple event fields. Using standard “and,” “or,” and “not” operators, you can define up to 15 event conditions.

NOTE: For more information on the event fields, see “Event Structure” in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al9m3w5.html).

After you define the filter criteria, you must select the object’s notification channel. Notification channels are simply the Channel objects the logging server uses to provide event notification. For example, if you want to e-mail filtered events to your mailbox, you must select an SMTP Channel object that is configured to relay events to your e-mail address. Similarly, if you want to log filtered events to a MySQL database, you must select a MySQL Channel object that is configured to write events to the correct database and table. You can define multiple notification channels for any given Notification Filter.

For information on creating and configuring Notification Filter objects, see “Configuring Notification Filters” on page 227.

Heartbeat Objects

Heartbeat objects define which Event IDs the logging server looks for and the interval at which those events must occur. If an event does not occur within the designated interval, the logging server generates a heartbeat event.

The heartbeat event is automatically logged to the central data store; however, if you want to receive notification that a specific event has not occurred, you must create a Notification Filter for the corresponding heartbeat event.

For information on creating and configuring Heartbeat objects, see “Configuring Heartbeat Objects” on page 229.

Notification Containers

The logging server only looks for Notification Filter and Heartbeat objects in Notification containers; therefore, Notification Filter objects can only be created within Notification containers.

Notification containers provide a reference point through which the logging server can locate Notification objects. At startup, the logging server scans its list of Notification containers and loads the included Notification object configurations in memory where it can quickly access the information to filter or monitor events. For information on configuring the Notification Container property on the logging server, see “Configuring the Secure Logging Server” on page 218.

IMPORTANT: The logging server only scans its list of Notification containers at startup. Therefore, if you create or modify a Notification object, you must restart the logging server. For information on restarting the logging server, see “Secure Logging Server Startup Commands” on page 320.

The Notification container under Logging Services is automatically created during installation; however, Notification containers can be created anywhere in the tree.

NetMail Attributes in Existing Directory Objects

When NetMail is installed, existing Directory objects, such as Container, User, and even Server objects, take on additional attributes. For complete explanations of the properties added to Container, User, and Server objects, see "NDS Object Configuration Options" on page 393.

NCP Server Objects

Description: Server Object icon

During installation, NetMail extends the definition of the NCP Server object to include the following properties:

- **Internet Mail** identifies the Messaging Server object associated with the current NCP Server object.
- **Syslog** is provided for backward compatibility only. In this page, administrators can define server-specific syslog files for NetMail 3.1 and earlier systems.

  IMPORTANT: In NetMail 3.5, all system logging is handled through Novell Nsure Audit.
- **Nsure Audit** has separate menus for NetWare, Filesystem, and eDirectory events. These properties manage the log settings for eDirectory, NetWare, traditional file system, and NSS events. Each menu lists the events that fall in its respective category. To configure the logging server to log a particular type of event, simply mark the event's check box and click Apply. Once you click Apply, the logging server automatically begins logging the marked events. For more information on configuring the NCP Server object's Nsure Audit attributes, see "Logging eDirectory, NetWare, and File System Events" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/all8rpn.html#all8rpn)

Container Objects

NetMail properties for Container objects include the option to define a custom message store for users within the current container and a container-specific domain name.

The container-specific message store is the volume and directory where the mailboxes for users in the current container are located. This does not affect the general message queue and SCMS directories, which are always located in the default message store volume and directory.

If configured, container domains appear in the From field of user messages and are referenced by the Address Book Agent in returning users' address book information.

IMPORTANT: Container domains do NOT allow you to have non-unique user IDs in different containers.

User Objects

Description: User Object icon

The NetMail attributes for User objects replicate many of the user configuration options available in the Modular Web client, including privacy level, forward and autoreply messages, and proxy configuration.

Providing the user configuration options in both the User object and Modular Web client gives administrators the option of centrally managing these options through the User object or allowing users to self-manage these options through the Modular Web client.

The User object also replicates many of the configuration options available in Parent objects.This duplication lets the administrator configure general settings in the Parent object, but create "exceptions to the rule" in individual User objects. For example, in the Parent object the administrator can set a mailbox quota for users in an Internet domain. However, at the User object level, the administrator can allocate a larger mailbox quota for the domain's Webmaster.

Message Processing

The core function of NetMail is message processing. Every message entering your messaging system—either inbound or outbound, from internal or external users—must be processed by NetMail agents. Depending on which agents are running on your messaging system, the message might be checked against a system blacklist, forwarded to another e-mail address, or filtered by user-defined rules.

The directory infrastructure that supports message processing comprises three basic components:

- Message Store
- Single Copy Message Store
- Message Queue

Everything that happens from the time a message enters the messaging system to when it is delivered to the user's mailbox occurs in these directories.

This section explains message processing both in terms of its directory infrastructure and the actual process. By understanding the internal structure of your NetMail system and how messages are processed, you can better manage your messaging system.

Message Store

The *message store* is the directory structure that holds users' mailboxes and messages. All other information required by your NetMail system is stored in eDirectory. Every server running an NMAP Agent has a message store. You can manually create additional message stores using Container objects or NetMail Parent objects. (See "Creating Separate Message Stores for Each Domain" on page 260.)

For information on mailbox file structure, see "Mailbox File Structure" on page 294.

Message Store Directory Structure

On a NetWare® server, the message store's default location is sys:\novonyx\mail. On a Windows server, the default location is \Program Files\novell\netmail\mail\. On a Linux* server, the default location is the /usr/nims directory.

NOTE: Because NetWare requires free space on the sys: volume, consider the potential disk space requirements of your messaging system before creating the mail directories on the sys: volume of a NetWare server. For information on changing the location of the message store, see the Message Store property in Table 4, "Configuring the NMAP Agent," on page 68.

The NMAP Agent creates the following mailbox directory structure within the message store directory for every User object in its assigned contexts:

netmail\	Initial directory for NetMail.
users\	Collective directory for all user mailboxes.
user_name\	A unique directory for each user's mailbox.
inbox.box	The file containing all messages in the user's InBox (text and attachments). New messages are appended to the end of the file.
inbox.idx	The index of all messages in the inbox.box file.
main.cal	The Main calendar store. This file contains calendar items such as tasks, appointments, and notes in the user's Main calendar.
main.idc	The index of all items in the main.cal file.
calendar_name.cal	The calendar store for any calendar other than the Main calendar. This file contains calendar items, such as tasks, appointments, and notes for the designated calendar.
calendar_name.idc	The index of all items in the *calendar_name*.cal file.
folder_name.box	A unique file for each folder in the user's mailbox. It contains the folder's messages (text and attachments). New messages are appended to the end of the file.
folder_name.idx	The index of all messages in the *folder_name*.box file.
folder_name\	A unique directory for each folder that contains subfolders. 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.
subfolder_name.box	A unique file for each subfolder in the parent folder. It contains the subfolder's messages (text and attachments). New messages are appended to the end of the file.
subfolder_name.idx	The index of all messages in the *subfolder_name*.box file.
shares\	A directory containing index files for the shared folders and calendars to which the current user has subscribed and has Mark Read or Delete rights. Local copies of the index files are not created if the user has Read Only rights.
shared_folder_name.sdx	The index of all messages in a shared folder to which the current user has subscribed. This local copy of the shared folder's index file allows the subscribed user to mark messages as read or delete messages without affecting the master copy of the shared folder.
shared_calendar_name.sdc	The index of all items in a shared calendar to which the current user has subscribed. This local copy of the shared calendar's index file allows the subscribed user to delete items without affecting the master copy of the shared calendar.

Single Copy Message Store

In cases when a message is sent to multiple recipients (by default, five or more) and the message is over 5 KB, NMAP does not replicate the message in all the users' mailboxes. Instead, a pointer message is sent to the individual mailboxes directing NMAP to the complete message in the

Single-Copy Message Store (SCMS) directory. When the last user downloads or deletes the message, it is deleted from the shared directory.

For more information, see "SCMS Message Structure" on page 294.

Single Copy Message Store Directory Structure

The SCMS directory structure stores messages in sorting directories that correspond to the last character in their hexadecimal filename (0-9 or A-F). Sorting messages by the last character in their hexadecimal filename allows the NMAP Agent to efficiently retrieve messages stored in the SCMS directories.

The SCMS directory structure is as follows:

netmail\	Initial directory for NetMail.
scms\	Single Copy Message Store (SCMS) directory.
0-9, a-f	Sorting directories. Messages are sorted in these directories by the last hash value in the SCMS filename.
xxxx	File with hashed filename (*xxxx* represents a hashed value) containing the multi-recipient message and any attachments.
xxxx.cnt	Counter file. Its value is the total number of recipients. As each recipient deletes the message, the counter file decrements by 1. When its value is 0, the message and counter files are deleted.

Message Queue

Each message store has an associated message queue. The message queue is the directory where messages are processed as they enter or leave your NetMail system.

For a complete discussion of how messages flow through the message queue, see "Message Processing in the Message Queue" on page 21.

Message Queue Directory Structure

The NMAP Agent is responsible for managing the message queue. When the NMAP Agent receives a message, it downloads the file to the following message queue directory:

netmail\	Initial directory for NetMail.
spool	Subdirectory for message queue

Message Processing in the Message Queue

As the NMAP Agent downloads a message to the message queue directory, it generates two files: c*xxxxxxx*.in and d*xxxxxxx*.in. (The *xxxxxxx* represents a hashed value of the date and time the message was sent. The .in extension indicates the message is inbound.)

The c*xxxxxxx*.* file is the control file envelope. The control file is generated from information received in the initial SMTP exchange. It contains To and From information along with any message flags. All message processing functions are performed on the control file.

The d*xxxxxxx*.* file is the data file. It contains the message header and message text. Because most message processing is done through the control file, the data file is rarely opened.

NOTE: For a complete breakdown of control file content and data file format, see Appendix B, “Message Structure,” on page 291.

After the message is downloaded, NMAP gives the data file a .msg extension and then begins moving the control file through eight queues. The process of moving the control file between queues is a simple matter of changing its filename extension to reflect the current queue number.

The following table outlines the message-processing functions associated with each queue.

xxxxxxxx.000	Queue 0: the prep queue. NMAP makes sure the control file meets all processing requirements and the AntiVirus Agent scans the data file.
xxxxxxxx.001	Queue 1: The message is processed by the AntiSpam Agent and/or the List Agent.
xxxxxxxx.002	Queue 2: The message is processed by the Alias Agent and/or the AutoReply Agent.
xxxxxxxx.003	Queue 3: The message is processed by the Rule Agent.
xxxxxxxx.004	Queue 4: This queue is not currently used by NetMail agents; it can be used by a third-party or custom agent.
xxxxxxxx.005	Queue 5: The message is processed by the Calendar Agent.
xxxxxxxx.006	Queue 6: Messages addressed to recipients within the messaging system are delivered by the NMAP Agent.
xxxxxxxx.007	Queue 7: Messages addressed to recipients outside the messaging system are picked up for delivery by the SMTP Agent.
xxxxxxxx.008	Queue 8: This queue is a holding queue for bounced messages. The NMAP Agent leaves bounced messages in queue 8 until it has time to reprocess them.

When the NMAP Agent moves a message into a queue, it notifies the agent registered on that queue. (Agents register on their queues when they first load.) The registered agent then scans the control file and performs its assigned function. If the agent modifies the message, NMAP returns the message to queue 0 for reprocessing. If no changes are made, NMAP advances the message to the next queue.

Message Processing: Step-by-Step Process

The following table provides a detailed, step-by-step breakdown of NetMail message processing. The outlined process includes all NetMail queue agents; however, on live systems the process includes only those agents actually loaded on messaging servers.

Table 2 Breakdown of NetMail Message Processing

Stage	Agent	Description
1	 User	Someone sends a message over the Internet to a user in your messaging system.

Stage	Agent	Description
2	 SMTP Agent	The SMTP Agent receives the message and transfers the message to its assigned NMAP Agent.
3	 NMAP Agent	In downloading the message to the message queue directory, the NMAP Agent creates the message control file (c*xxxxxxx*.in) and data file (d*xxxxxxx*.in). The control file contains To and From information along with any message flags. The data file contains the complete message. (See Appendix B, “Message Structure,” on page 291 for more information on the control file and data file.)
4	 NMAP Agent  AntiVirus Agent	After the message is downloaded, the NMAP Agent gives the data file a .msg extension and moves the control file to queue 0 by changing the file extension from .in to .000. In queue 0, the NMAP Agent verifies that the control file meets all processing requirements. It then notifies the AntiVirus Agent that it has a message to process. The AntiVirus Agent then scans the data file for any attachments. Attachments are sent to a third-party virus engine to be scanned. If an attachment contains a virus, the message is deleted from the queue. Depending on how the AntiVirus Agent is configured, it might send a virus alert to the message recipient or return the message to the sender. The NMAP Agent then moves the control file to queue 1 by changing the file extension from .000 to .001 and notifies the AntiSpam and/or List Agents that they have a message to process.
5	 AntiSpam Agent  List Agent	Queue 1 is shared by the AntiSpam Agent and the List Agent because it doesn’t matter which of these agents processes the message first. The AntiSpam Agent checks the control file to see if the sender is on its blackout list. If the sender is on the blackout list, the message is deleted from the queue. Depending on how the AntiSpam Agent is configured, it might return the message to the sender or send the Postmaster a copy of the returned message. The List Agent checks the control file to see if the message is addressed to a mailing list. If it is, the List Agent generates a new message with the names of the individual users in the mailing list. The new message is returned to queue 0 and the original message is deleted.
6	 NMAP Agent	If there are no changes, the NMAP Agent moves the file to queue 2 by changing the file extension from .001 to .002 and notifies the Alias and/or AutoReply Agents that they have a message to process.
7	 Alias Agent  AutoReply Agent	Queue 2 is shared by the Alias Agent and the AutoReply Agent because it doesn’t matter which of these agents processes the message first. The Alias Agent checks the control file to see if the recipient matches any of its defined aliases. If so, the Alias Agent replaces the alias with its corresponding e-mail address. The AutoReply Agent checks the recipient’s User object to see if the recipient has either configured an autoreply message or forwarded messages to another e-mail account. (The user’s forward and autoreply information is stored in his or her User object.) If the recipient has forwarded his or her mail, the agent adds the forwarded address to the recipient list. If the recipient did not request a copy of the message, the agent replaces the recipient’s name with the forwarded address. If the recipient has configured an autoreply message, the agent generates a new message and hands it off to NMAP for processing in the message queue.

Stage	Agent	Description
8	 NMAP Agent	If the original message has been modified, the NMAP Agent returns the message to queue 0 for reprocessing. If there are no changes, the NMAP Agent moves the file to queue 3 by changing the file extension from .002 to .003 and notifies the Rule Agent that it has a message to process.
9	 Rule Agent	In queue 3, the Rule Agent checks the message against the recipient's defined rules. (Rules are stored in the user's User object.) If the message matches one of the rule conditions, the Rule Agent applies the rule. If a rule moves the message to a specific folder, the Rule Agent adds the destination folder information to the control file in IMAP format. Using the IMAP protocol to designate the destination folder enables the message to be routed to the correct folder in any standards-based e-mail client.
10	 NMAP Agent	If the message has been modified, the NMAP Agent returns the message to queue 0 for reprocessing. If there are no changes, the NMAP Agent moves the file to queue 5 by changing the file extension from .003 to .005. (Queue 4 is not currently used by NetMail agents although it can be used by third-party or custom agents.)
11	 Calendar Agent	In queue 5, the Calendar Agent checks to see if the message is an Accept or Decline reply to a scheduled appointment. If the message is a response to an appointment and if the person who scheduled the appointment is a local user, the Calendar Agent updates the user's calendar store (mail.cal) to indicate the sender accepted or declined the appointment.
12	 NMAP Agent	If the original message has been modified, the NMAP Agent returns the message to queue 0 for reprocessing. If there are no changes, the NMAP Agent moves the file to queue 6 by changing the file extension from .005 to .006.
13	 NMAP Agent	In queue 6, the NMAP Agent checks the recipient list in the control file envelope; it then performs one of the following actions: ◆ If any of the recipients are local users, the NMAP Agent delivers a copy of the message to the users' mailboxes. See "Message Store Directory Structure" on page 19. ◆ If the message exceeds the Single Copy Message Store (SCMS) threshold, the message is copied to the SCMS directory. See "Single Copy Message Store" on page 20. ◆ If some of the recipients are not in the current NMAP Agent's context but are within the Directory tree, the NMAP Agent transfers the message to the NMAP Agents assigned to the users' contexts. ◆ If any recipients are not within the Directory tree, the NMAP Agent moves the message to queue 7 for remote delivery.
14	 NMAP Agent	In queue 7, the NMAP Agent passes the message to the SMTP Agent for remote delivery.

Message Processing Performance

NetMail processes messages very rapidly. The NMAP Agent is multi-threaded and can simultaneously process as many messages as memory will allow. To ensure optimal efficiency, NetMail includes a Mail Load utility that balances the NMAP Agent's thread usage with server utilization.

Magnifying the efficiency of the NMAP Agent, NetMail's message processing is strategically designed to optimize performance. For example, separating each message into a control file and a data file speeds performance because most message processing is done using the small, compact control file. The larger data file is rarely opened.

The message queue itself is also designed for speed. Changing the control file's extension in a single directory rather than transferring the file between different queue directories makes advancing through the queue as efficient as possible.

Finally, having NMAP notify agents when a message is placed in their queues, rather than having the agents periodically scan their queues, means there is zero wait time between message-processing functions.

2 Planning Your NetMail System

This section reviews the basic Novell® NetMail™ configurations and their related Novell eDirectory™ requirements. It helps you decide the NetMail configuration that best suits your organization's needs and how to implement that configuration.

Section topics include

- "Understanding How NetMail and eDirectory Work Together" on page 27
- "Selecting Your NetMail System Configuration" on page 28
- "Planning Your System Implementation" on page 29
- "Building Fault Tolerance in NetMail" on page 41

Understanding How NetMail and eDirectory Work Together

Because NetMail is completely integrated with eDirectory, you must plan your NetMail system around the inherent requirements of eDirectory.

Foremost among these requirements is eDirectory access. NetMail uses eDirectory exclusively to store and look up user information and system configuration parameters. In fact, the only things not stored in eDirectory are the messages. Consequently, the speed that eDirectory can retrieve or store information heavily impacts NetMail's performance.

To minimize messaging server reaction time and ensure high system performance,

- Every messaging server must have local access to its corresponding Message Server object in eDirectory.
- Every NMAP server requires local access to all User objects within its assigned contexts (that is, those User objects with a mailbox directory on the server).

These two requirements must be met for optimal performance in any NetMail messaging system.

Optimizing eDirectory for NetMail

To give the messaging server and NMAP Agent local access to their associated objects, the Directory can be copied—or in NetWare® terms, replicated—on each messaging server. By default, NetWare automatically replicates the entire Directory on the first three servers in the tree. To give subsequent servers local access to eDirectory data, manually replicate the Directory to those servers. For information on Directory replication, see Replicas in the Novell eDirectory 8.7.1 Administration Guide (http://www.novell.com/documentation/lg/edir871/index.html?page=/documentation/lg/edir871/edir871/data/fbaecheh.html).

Although replication gives servers local access to eDirectory data, it also generates significant network traffic. Each time there is a change in the Directory, that change must be synchronized on every replica. Depending on the number of objects in the Directory, network speed, and server

resources, synchronizing each replica can consume your network bandwidth and drag down system performance.

To make system synchronization more manageable, you can replicate only those portions of the Directory needed by each messaging server. eDirectory allows you to break the Directory into sections called partitions; therefore, instead of replicating the entire Directory, you can replicate only those partitions that contain the messaging servers' associated objects. For information on NetWare partitions, see Partitions in the Novell eDirectory 8.7.1 Administration Guide (http://www.novell.com/documentation/lg/edir871/index.html?page=/documentation/lg/edir871/edir871/data/fbachabc.html).

To better understand how to ensure that each messaging server has local access to its associated objects, consider your eDirectory configuration in context of your NetMail system. The following sections review the five basic NetMail system types and their associated configuration requirements.

Selecting Your NetMail System Configuration

In general, NetMail messaging systems fall into one of five configurations:

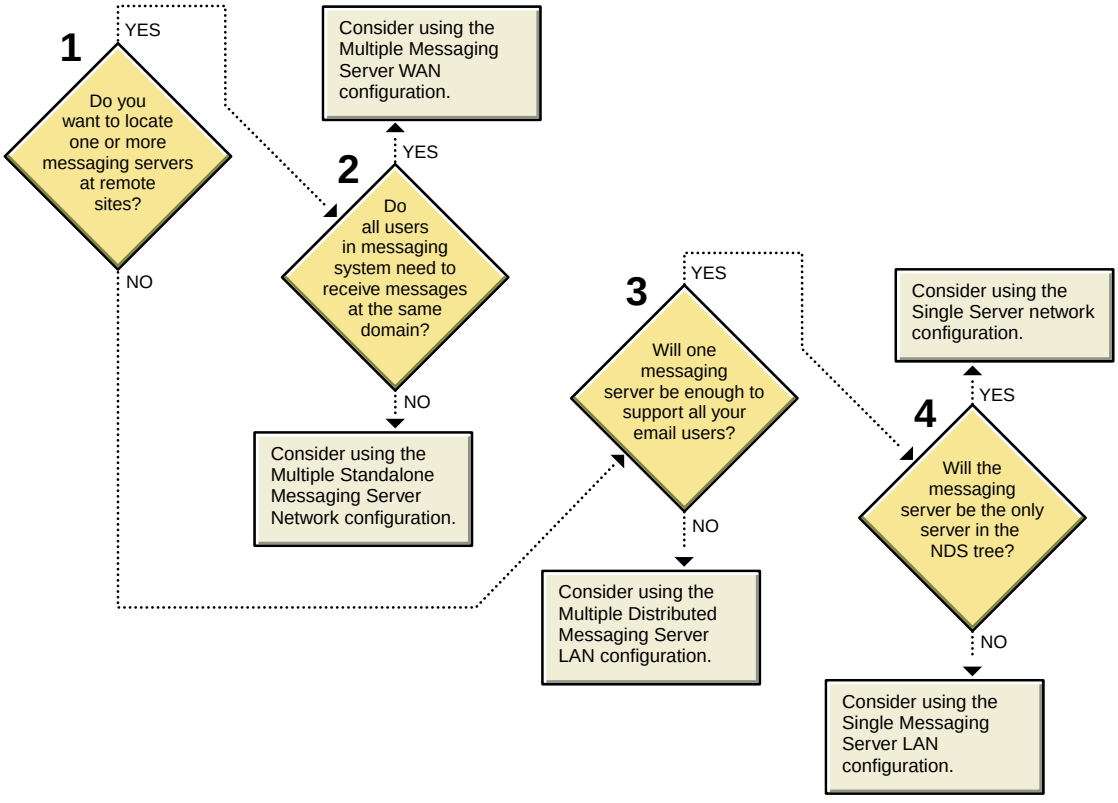
Table 3 Five NetMail System Configurations

Configuration	Description
Single Server Network	The single server network is the most simple NetMail configuration because the NetMail messaging server is the only server in the Directory tree. This configuration is typically used by small to medium organizations that do not use eDirectory for other network services.
Single Messaging Server LAN	The single messaging server LAN is a system with more than one server in the Directory tree; however, only one server provides messaging services. This configuration is typically used by small to medium organizations that do not use eDirectory for other network services.
Multiple Standalone Messaging Server LAN	A multiple standalone messaging server LAN is a network with multiple messaging servers, but each messaging server has its own Internet domain name—that is, the users serviced by each messaging server receive messages at a unique domain. This configuration is typically used by medium to large organizations that have several, separately managed IS departments and Internet domains or subdomains.
Multiple Distributed Messaging Server LAN	A multiple distributed messaging server LAN is a network with multiple messaging servers that work together to provide messaging services. This configuration is typically used by ISP, ASP, or medium to large LAN environments in which message traffic exceeds the resources of a single server, but all the messaging servers share the same high-speed network.
Multiple Messaging Server WAN	A multiple messaging server WAN is a network in which the messaging system connects different geographical locations, but users still receive messages at the same Internet domain. This configuration is typically used by government and enterprise organizations that have one or more remote locations.

What Configuration Is Right for You?

If you are unsure what configuration to implement, use the following flow chart to help you decide:

Description: Flow chart to decide the messaging system configuration right for your organization



Planning Your System Implementation

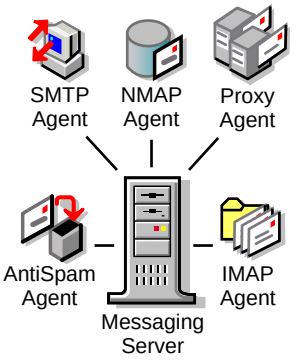
After selecting your NetMail system but before the installation, review the configuration requirements associated with your messaging system The following section reviews the configuration requirements for each of the NetMail system types.

- Single Server Network
- Single Messaging Server LAN
- Multiple Standalone Messaging Server LAN
- Multiple Distributed Messaging Server LAN
- Multiple Messaging Server WAN

Single Server Network

For a single server network, your initial NetMail installation is your complete messaging system.

Description: Single Server Network Configuration



Although a single server tree is very simple in its configuration, such a system is capable of providing efficient messaging services for xx250,000 to 350,000xx users.

NOTE: For a practical example of this configuration, see "Single Server Network" on page 283.

Messaging System Configuration

You can automatically create your messaging server's agents during NetMail installation, or you can manually create those agents after installation. In either case, plan the agent services you want to provide to your users.

NOTE: For an overview of each agent's function, see "NetMail Agents" on page 8. For a detailed explanation of each agent's configuration options, see Appendix H, "NetMail Configuration," on page 343.

eDirectory Configuration

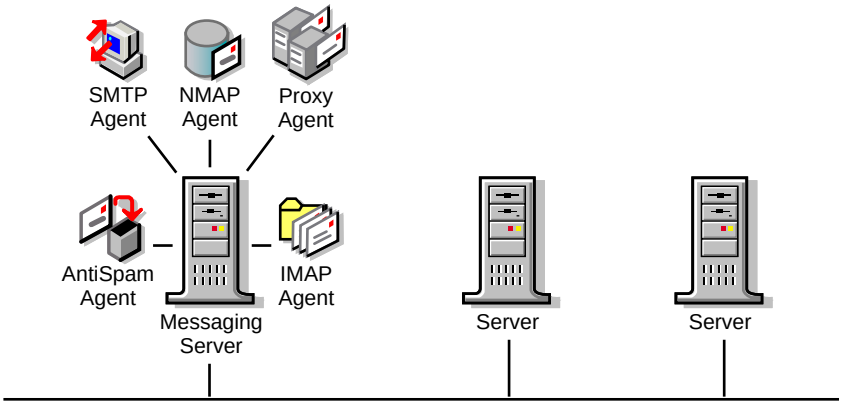
Because the entire Directory tree resides on a single machine, the messaging server automatically has local access to the Messaging Server object and all User objects in the tree. Therefore, no additional Directory configuration is necessary.

Single Messaging Server LAN

In a single messaging server system, a dedicated messaging server is integrated with an organization's existing multiple-server, Directory-based 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 leverage objects that already exist in eDirectory.

Like the single server network, your initial NetMail installation is your complete messaging system.

Description: Single Messaging Server LAN Configuration



NOTE: For a practical example of this configuration, see "Single Messaging Server LAN" on page 284.

Messaging System Configuration

During a standard NetMail installation, you can automatically create your messaging server's agents or you can manually create those agents after installation using WebAdmin. In either case, plan the agent services you want to provide to your users.

NOTE: For an overview of each agent's function, see "NetMail Agents" on page 8. For a detailed explanation of each agent's configuration options, see Appendix H, "NetMail Configuration," on page 343.

eDirectory Configuration

Because multiple servers exist on the network, the messaging server does not automatically have local access to the Messaging Server object or the messaging system's User objects.

To give the messaging server local access to the Messaging Server object and all messaging system User objects, you must do the following:

- Create a read/write replica of a partition containing the Internet Services container on the messaging server (Internet Services contains the Messaging Server object).

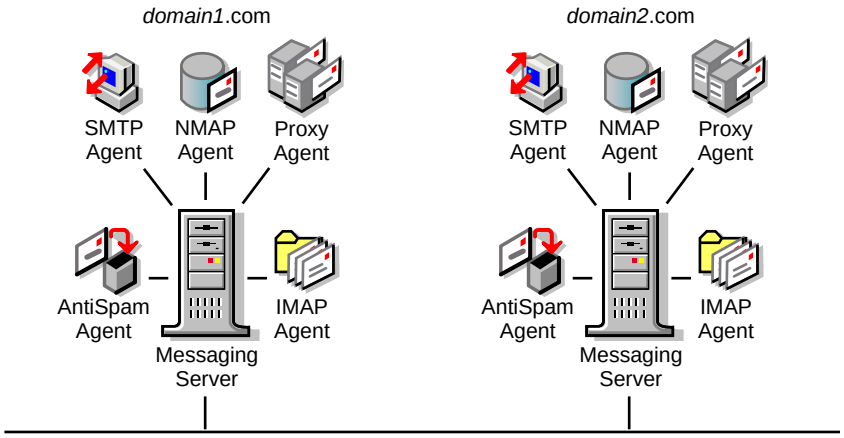
  By default, the root partition contains the Internet Services container. However, if you do not want to replicate the entire root partition on the messaging server, create a separate partition for the Internet Services container.

- Create a read/write replica of all partitions containing messaging system User objects on the NetMail messaging server.

Multiple Standalone Messaging Server LAN

In this system, multiple messaging servers are in use, but each messaging server is assigned to a different domain and functions as an independent messaging system.

Description: Multiple Standalone Messaging Server LAN



NOTE: For a practical example of this configuration, see "Multiple Standalone Messaging Server LAN" on page 285.

Messaging System Configuration

In configuring a multiple standalone message server LAN, you must do the following:

- Install NetMail on each messaging server.
- Create each Messaging Server object.
- Turn off distributed processing.
- Create and configure NetMail agents.

Each of these steps is outlined in the following sections.

Installing NetMail on Each Messaging Server

When you install NetMail on your first messaging server, the eDirectory schema is extended to include NetMail-specific objects. This is the only time you need to extend the schema.

Therefore, before installing NetMail on additional messaging servers, allow time for the schema extensions to synchronize throughout the entire tree. Then, when installing NetMail on subsequent servers, select *only* Novell NetMail Files in the list of installation options. This option installs the messaging system files to the server but does not re-extend the schema.

Do not select Configure Server for NetMail because this option automatically creates the Messaging Server object in the Internet Services container. To provide an intuitive distribution of objects in a Multiple Standalone Messaging Server LAN, you typically want to create each Messaging Server object in the container associated with its User objects.

NOTE: For further information on NetMail installation options and installing NetMail, see Chapter 3, "Installing NetMail 3.5," on page 45.

Creating Messaging Server Objects

After installing the NetMail files on each messaging server, you need to create the servers' associated Messaging Server objects.

Create each Messaging Server object in the same container as its users. Standalone messaging servers are typically created in the containers associated with their User objects for the following reasons:

- It is administratively intuitive.

- It simplifies rights management because administrators only need to have rights to the containers they are responsible.
- Simple administrative tasks, such as adding users, you can delegate on a container basis.
- If a standalone messaging server is located in the Internet Services container, it actually functions as a partially non-distributed server. While it is not able to locate or communicate with other messaging servers, distributed messaging servers are still able to locate and forward messages to it.
- Instead of replicating both the Internet Services and User object partitions to every messaging server, you only need to replicate the messaging servers' associated container partitions.

NOTE: For more information, see "Messaging Server" on page 59.

Turning Off Distributed Processing

By default, messaging servers search the tree for the Internet Services container and its associated Messaging Server objects. This "distributed processing" enables multiple messaging servers to function as a single, integrated system.

In standalone messaging systems, however, messaging servers do not interact with each other. Instead, each messaging server functions as an independent messaging system, exclusively providing all NetMail services to the users within its assigned contexts.

To prevent messaging servers from searching the tree for Internet Services and its associated Messaging Server objects, mark the Distributed Processing Disabled option in the Messaging Server object Identification page.

NOTE: For more information on this option, see the Distributed Processing Disabled property in the Messaging Server object.

Creating and Configuring NetMail Agents

Because standalone messaging servers function independently of each other, they must have all the NetMail agents required for a self-contained messaging system.

At a very minimum, each messaging server must have the following agents:

- NMAP
- SMTP
- A client agent (POP, IMAP, or the Modular Web Agents)

The additional agents you can add depend on the services you want to provide to your users.

The NMAP, SMTP, POP, IMAP, Modular Web Agent, AutoReply, Rule, Proxy, Alias, AntiSpam, AntiVirus, List, and Connection Manager agents must run locally on standalone messaging servers.

If you run the Address Book Agent on a standalone messaging server, it only returns local users in address book queries. To provide a system-wide address book, you can run the Address Book Agent on a central distributed messaging server and configure the local e-mail clients to access the distributed Address Book Agent as an LDAP server.

NOTE: For an overview of each agent's function, see "NetMail Agents" on page 8. For a detailed explanation of each agent's configuration options, see Appendix H, "NetMail Configuration," on page 343.

eDirectory Configuration

Because multiple servers exist on the network, each messaging server does not automatically have local access to its Messaging Server or assigned User objects.

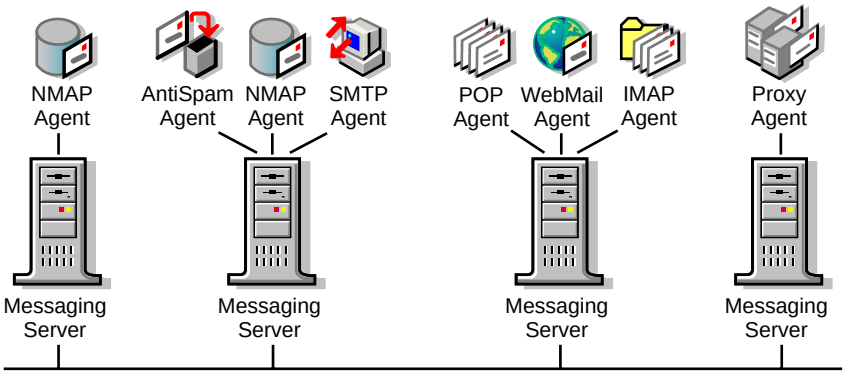
To give the messaging server local access to its Messaging Server and User objects, create a read/write replica of the partition containing the Messaging Server object and its associated User objects on the messaging server.

Multiple Distributed Messaging Server LAN

A multiple distributed messaging server LAN is a common ISP, ASP, or multi-LAN configuration. Due to the volume of messages handled by the messaging system, performance requirements, or the local distribution of the network, NetMail components are distributed over several messaging servers.

In such environments, you can configure two or more messaging servers to work together as a single, integrated system. In this way, messaging system functions are distributed across multiple servers to provide load balancing, fault tolerance, and speed. For a review of agent distribution strategies, see "Creating and Configuring NetMail Agents" on page 33.

Description: Multiple Distributed Messaging Server LAN



NOTE: For a practical example of this configuration, see "Multiple Distributed Messaging Server LAN" on page 286.

Messaging System Configuration

In configuring a multiple distributed message server LAN, you must do the following:

- Install NetMail on each messaging server.
- Create each Messaging Server object.
- Create and configure NetMail agents for each messaging server.
- Configure trusted hosts.

Each of these steps is outlined in the following sections.

Installing NetMail on Each Messaging Server

When you install NetMail on your first messaging server, the eDirectory schema is extended to include NetMail-specific objects. This is the only time you need to extend the schema.

Therefore, before installing NetMail on additional messaging servers, allow time for the schema extensions to synchronize throughout the entire tree. Then, when installing NetMail on subsequent servers, select *only* Novell NetMail Files in the list of installation options. This option installs the messaging system files to the server but does not re-extend the schema.

NOTE: You can also select Configure Server for NetMail if you want to create your Messaging Server objects during the installation.

For further information on NetMail installation options and installing NetMail, see Chapter 3, "Installing NetMail 3.5," on page 45.

Creating Messaging Server Objects

After installing the NetMail files on each messaging server, you need to create the servers' associated Messaging Server objects.

Typically, distributed messaging servers are created in the Internet Services container because distributed messaging servers search the tree for that container and its associated Messaging Server objects. Looking for other messaging servers in Internet Services enables distributed servers to share agents and message processing functions.

It is possible, however, to create a Messaging Server object outside the Internet Services container and have it function in distributed mode if you create an Alias object for it within Internet Services. Alias objects enable distributed messaging servers to locate and interact with messaging servers outside the Internet Services container in the same way they interact with messaging servers inside the Internet Services container. For more information, see "Messaging Server" on page 59.

NOTE: You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Internet Services container.

Creating and Configuring NetMail Agents

In planning your distributed messaging system, you need to decide the agent services you want to provide to your users and how to distribute those agents.

In part, agent distribution depends on the server resources required for any given service and its volume of usage. For example, in messaging systems with a high volume of e-mail client usage, you might want to run the POP, IMAP, and Modular Web Agents on a dedicated, high-performance e-mail server. Or, in environments with heavy proxy usage, you can create a dedicated Proxy server and configure the Proxy Agent to query its user accounts every hour.

Another point to consider in agent distribution is fault tolerance. Identify your most critical services and distribute those agents accordingly. For example, to insulate your messaging system from denial-of-service attacks, you can run the SMTP Agent with an NMAP Agent on a dedicated server. If you assign the NMAP Agent a context without any users, its sole function is to handle all incoming SMTP messages. Therefore, in the event of a SPAM attack, no users are impacted and the remaining NMAP Agents are free to continue processing and delivering messages.

NOTE: For more information on providing fault tolerance through agent distribution, see "Application-Level Clustering" on page 42.

Finally, in planning agent distribution, you must consider the message path. In systems with multiple NMAP Agents, it is possible that a message is processed twice on its way from the queue server to the message store. To avoid reprocessing messages, you must do the following:

- First, manage queue server and message store functions on different NMAP servers. This means that the queue server (i.e., the NMAP Agent to which the SMTP, Modular Web, and Proxy Agents deliver messages that the message queue needs to process) cannot have any users in its assigned context. Likewise, do not use the message store (i.e., the NMAP Agent that manages the user's mailboxes) as a queue server.

- Secondly, configure each agent to monitor either the queue server or the message store, but not both. This ensures that no agent is processing messages at both ends of the message path.

NOTE: For an overview of each agent's function, see "NetMail Agents" on page 8. For a detailed explanation of each agent's configuration options, see Appendix H, "NetMail Configuration," on page 343.

Configuring Trusted Hosts

When NetMail agents need to access 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 all agents running on other servers (including other NMAP Agents) to authenticate with the server before the NMAP Agent carries out their requests.

As trusted hosts, agents are not required to authenticate with the NMAP server. Rather, they are given open access to the NMAP Agent and its accompanying message queues and mail directories.

Assigning trusted host status to NetMail agents typically improves system performance because the NMAP Agent can skip the authentication process in server-to-server agent transactions.

On Linux servers, however, do not grand trusted host status unless login access to trusted host servers is restricted to the system administrator.

NOTE: Trusted hosts are configured through the NMAP Agent. For more information, see the Trusted Hosts property in Table 4, "Configuring the NMAP Agent," on page 68.

eDirectory Configuration

Because multiple servers exist on the network, each messaging server does not automatically have local access to the Messaging Server object and every NMAP server does not have local access to all User objects within its assigned contexts (i.e., those User objects with a mailbox directory on the server).

To give every messaging server local access to its Messaging Server object, create a read/write replica of a partition containing the Internet Services container on each messaging server (Internet Services contains all distributed Messaging Server objects).

By default, the root partition contains the Internet Services container. However, if you do not want to replicate the entire root partition on the messaging server, create a separate partition for the Internet Services container.

To give each NMAP server local access to its assigned User objects, create a read/write replica of all partitions containing the NMAP Agent's assigned User objects on the NMAP server.

Multiple Messaging Server WAN

A multiple messaging server WAN 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 do not grand trusted host status work together without generating unnecessary network traffic across the slow WAN connections.

In designing WAN messaging systems, first consider the links that exist between offices. For locations that connect to the central office or the central messaging server over fast links, employ the same strategies as in a regular distributed messaging server environment.(See "Multiple Distributed Messaging Server LAN" on page 34.) However, locations that connect to the central office over slow links must use a different strategy.

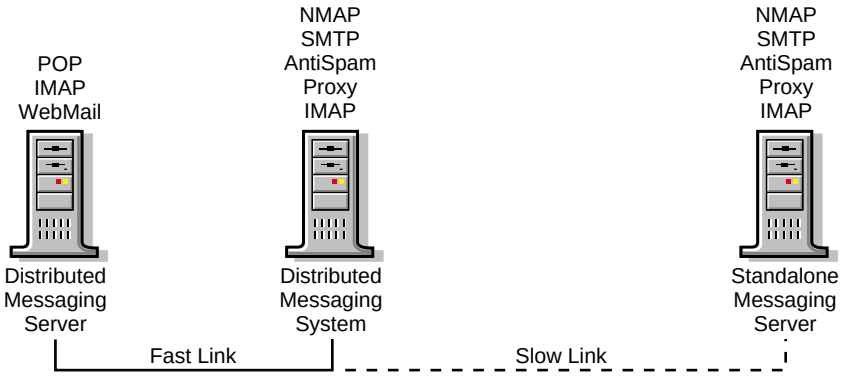
In slow-link WAN environments, it doesn't make sense to replicate both the Internet Services and User object partitions on every messaging server. While this configuration optimizes performance in LAN environments, replicating multiple partitions across slow links can jam the connection and slow the network to a crawl.

Another concern in slow-link environments is preventing messaging servers in remote offices from searching the Directory tree for the Internet Services container and User objects that are not replicated at the remote location. Searching the tree over a slow link not only increases network traffic, but it can compromise the functionality of the system. If the eDirectory query times out before it is able to receive the needed information, NetMail continues to query other replicas until your server resources are exhausted.

One way of addressing these concerns is to locate all messaging servers at the central office. Users in remote locations then need to access messaging servers across the WAN. While functional, this option does not provide optimal performance. Users in remote locations might experience perceivably slow service as they wait to send and download mail over the slow link.

A better solution is to provide standalone messaging servers at each remote location. Network traffic is reduced because all messaging operations take place on the local standalone server and, because the standalone messaging server is in the users' local environment, users experience faster service when using their e-mail clients (actual message delivery time does not change for messages that traverse the WAN).

Description: Multiple Messaging Server WAN



NOTE: For a practical example of this configuration, see "Multiple Messaging Server WAN" on page 288.

Messaging System Configuration

In configuring a multiple standalone message server WAN, you must do the following:

- Configure the WAN's distributed messaging servers.
- Install NetMail on the remote messaging servers.
- Create each remote Messaging Server object.
- Turn off distributed processing.
- Create and configure NetMail agents.
- Forward local undeliverable messages.
- Create an alias for each remote Messaging Server object.
- Configure trusted hosts.

Each of these steps is outlined in the following sections.

Configuring the WAN's Distributed Messaging Systems

WAN environments are heterogeneous messaging systems. While slow-link offices require standalone messaging systems, the WAN still needs at least one distributed messaging server to maintain a replica of the complete messaging system and to route messages between standalone systems. Furthermore, offices that connect to the central office over fast links can support distributed messaging servers.

In deploying a WAN-based messaging system, deploy your distributed messaging servers before the standalone messaging servers. Depending on message traffic volume, performance requirements, and network distribution, you might only need a single distributed messaging server for your central office. In this case, follow the configuration guidelines for a single messaging server LAN. (See "Single Messaging Server LAN" on page 30.)

If your central office requires multiple distributed messaging servers or if you are deploying distributed messaging servers in offices with fast links, follow the configuration guidelines for multiple distributed messaging server LANs. (See "Multiple Distributed Messaging Server LAN" on page 34.)

Installing NetMail on Remote Messaging Servers

After installing NetMail on your distributed messaging servers, then install NetMail on your remote servers.

At the time you installed NetMail on your first distributed messaging server, the eDirectory schema was extended to include NetMail-specific objects. This is the only time you need to extend the schema.

Therefore, before installing NetMail on remote messaging servers, allow time for the schema extensions to synchronize throughout the entire tree. (This can take some time in WAN environments.) Then, when installing NetMail, select *only* Novell NetMail Files in the list of installation options. This option installs the messaging system files to the server but does not re-extend the schema.

Do not select Configure Server for NetMail. This option automatically creates the Messaging Server object in the Internet Services container. In creating a multiple messaging server WAN, you must create each standalone Messaging Server object in the same container as its users.

NOTE: For further information on NetMail installation options and installing NetMail, see Chapter 3, "Installing NetMail 3.5," on page 45.

Creating Remote Messaging Server Objects

After NetMail is installed on each remote messaging server, you need to create the servers' associated Messaging Server objects.

To create the remote systems' Messaging Server objects,

Create each Messaging Server object in the same container as its users.

Standalone messaging servers are typically created in the containers associated with their User objects for the following reasons:

- It is administratively intuitive.
- It simplifies rights management because administrators only need to have rights to the containers for which they are responsible.

- Simple administrative tasks, such as adding users, you can delegate on a container basis.
- If a standalone messaging server is located in the Internet Services container, it actually functions as a partially non-distributed server. While it is not able to locate or communicate with other messaging servers, distributed messaging servers are still able to locate and forward messages to it.
- Instead of replicating both the Internet Services and User object partitions to every messaging server, you only need to replicate the messaging servers' associated container partitions.

In creating each Messaging Server object, type the messaging system's domain name in the Official Domain Name field of the Create Messaging Server dialog.

NOTE: For more information, see "Messaging Server" on page 59.

Turning Off Distributed Processing

By default, messaging servers search the tree for the Internet Services container and its associated Messaging Server objects. This "distributed processing" enables multiple messaging servers to function as a single, integrated system.

In standalone messaging systems, however, messaging servers do not interact with each other. Instead, each messaging server functions as an independent messaging system, exclusively providing all NetMail services to the users within its assigned contexts.

To prevent messaging servers from searching the tree for Internet Services and its associated Messaging Server objects, mark the Distributed Processing Disabled option in the Messaging Server object Identification page.

NOTE: For more information on this option, see the Distributed Processing Disabled property in the Messaging Server object.

Creating and Configuring NetMail Agents

Because standalone messaging servers function independently of each other, they must have all the NetMail agents required for a self-contained messaging system.

At a very minimum, each messaging server must have the following agents:

- NMAP
- SMTP
- A client agent (POP, IMAP, or the Modular Web Agents)

The additional agents you add depends on the services you want to provide to your users.

The NMAP, SMTP, POP, IMAP, Modular Web Agent, AutoReply, Rule, Proxy, Alias, AntiSpam, AntiVirus, List, and Connection Manager agents must run locally on standalone messaging servers.

If you run the Address Book Agent on a standalone messaging server, it only returns local users in address book queries. To provide a system-wide address book, you can run the Address Book Agent on a distributed messaging server and configure the local e-mail clients to access the distributed Address Book Agent as an LDAP server.

NOTE: For an overview of each agent's function, see "NetMail Agents" on page 8. For a detailed explanation of each agent's configuration options, see Appendix H, "NetMail Configuration," on page 343.

Forwarding Local Undeliverable Messages

When 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 messages over the Internet. However, they cannot send messages to or receive messages from colleagues in other offices within their messaging system domain.

To enable users in remote locations to send messages to users in other offices, you must configure each remote messaging server to forward local undeliverable messages. Local undeliverable messages are messages that are addressed to the messaging system domain, but whose recipients are not 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 in this local messaging system.

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.

In WAN environments, you must configure each remote NMAP Agent to forward local undeliverable messages to the central distributed messaging server.

NOTE: For more information, see the Forward Local Undeliverable Messages property in Table 4, "Configuring the NMAP Agent," on page 68.

Creating an Alias for Each Remote Messaging Server Object

With the Forward Local Undeliverable Messages option configured for each remote NMAP Agent, the remote messaging servers 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 central distributed messaging server still cannot send messages to remote messaging servers 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.

To enable the central distributed messaging server to route messages to remote messaging servers, each remote messaging server must have a corresponding Alias object in the Internet Services container.

NOTE: You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Internet Services container.

With the Forward Local Undeliverable Messages option configured on every remote messaging server and with each Messaging Server object (both distributed and standalone) represented in the Internet Services container, the messaging system is now fully functional.

To summarize:

- Remote users can send messages to users throughout the messaging system because the NMAP Agent on each remote messaging server is configured to send local undeliverable messages to a central distributed messaging server. The distributed messaging server can then route these messages to the appropriate NMAP Agent.
- Remote users can receive messages from users throughout the messaging system because an Alias object representing each standalone Messaging Server object is created in the Internet

Services container. These Alias objects enable distributed messaging servers to locate and route messages to standalone messaging servers.

Configuring Trusted Hosts

When NetMail agents need to access 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 all agents running on other servers (including other NMAP Agents) to authenticate with the server before the NMAP Agent carries out their requests.

Because the NMAP Agent on the central distributed messaging server routes messages between standalone systems, it needs trusted host status to every remote messaging server's NMAP Agent.

As a trusted host, the central NMAP Agent is not required to authenticate with the remote messaging servers. Rather, it is given open access to the remote NMAP Agents and their accompanying message queues and mail directories. This typically improves system performance because the messaging server can skip the authentication process in these NMAP-to-NMAP Agent transactions.

On Linux servers, however, do not grand trusted host status unless login access to trusted host servers is restricted to the system administrator.

NOTE: Trusted hosts are configured through the NMAP Agent. For more information, see the Trusted Hosts property in Table 4, "Configuring the NMAP Agent," on page 68.

eDirectory Configuration

Because multiple servers exist on the network, the remote messaging servers do not automatically have local access to their Messaging Server or assigned User objects.

To give each remote messaging server local access to its Messaging Server and User objects, create a read/write replica of the partition containing the Messaging Server object and its associated User objects on the messaging server.

All distributed messaging servers must have local access to their associated Messaging Server objects and every distributed NMAP server must have local access to all User objects within its assigned contexts (i.e., those User objects with a mailbox directory on the server).

To give every distributed messaging server local access to its Messaging Server object, create a read/write replica of a partition containing the Internet Services container on each messaging server (Internet Services contains all distributed Messaging Server objects).

By default, the root partition contains the Internet Services container. However, if you do not want to replicate the entire root partition on the messaging server, create a separate partition for the Internet Services container.

To give each distributed NMAP server local access to its assigned User objects, create a read/write replica of all partitions containing the NMAP Agent's assigned User objects on the NMAP server.

Building Fault Tolerance in NetMail

Because e-mail, scheduling, address books, and calendars are mission-critical applications, system reliability is one of the most important aspects of any messaging system. Indeed, 99.99% uptime requirements are not uncommon. System fault tolerance is achieved when there is no single point of failure in the system; that is, if any one server fails, mail users are unaffected.

In NetMail, redundancy and failover support you can implement at two levels: the application level and the hardware level.

Application-Level Clustering

Application-level clustering consists of duplicating mail services on multiple servers. Due to NetMail's highly modular architecture and eDirectory™ replication, critical services can run simultaneously on multiple servers and provide the exact same service. Consequently, you can provide fault tolerance for most mail services at the application level.

In comparison to hardware-level clustering, application-level clustering is relatively inexpensive. It is innate to NetMail 3.5 and does not require specialized hardware. In fact, servers in a NetMail application cluster do not even need to run the same operating system. As an added benefit, application clustering automatically provides load balancing because you can have all servers active at all times in a NetMail application cluster. Consequently, application-level clustering is the first choice in building system fault tolerance to use wherever possible.

Client Agents

NetMail client agents (POP, IMAP, ModWeb) provide the exact same service regardless of the server on which they reside. Therefore, you can configure these agents to run on as many servers as needed to handle messaging traffic and provide fault tolerance.

NOTE: To simplify administration in cluster environments, Novell Cluster Services allows you to create a virtual Server object that represents the cluster. The virtual Server object provides a single point of configuration for multiple servers with identical configurations.

Load balancing is achieved with round-robin DNS or with level 4 switching. Round-robin DNS resolves one host name to multiple IP addresses. The IP addresses that the DNS server returns are rotated so one IP address is not preferred.

Level 4 switching distributes the traffic sent to one IP address to multiple IP addresses. Some level 4 switches have advanced features that recognize when one IP address is not responding and automatically direct client requests to the remaining servers.

IMPORTANT: If using ModWeb behind a level 4 switch, the switch must also guarantee that all requests coming from a single IP address are always redirected to the same server. This is necessary because ModWeb maintains session information on the server. (The POP and IMAP Agents do not have this restriction.)

SMTP and the Mail Queue

Fault tolerance is built into the SMTP protocol. Consequently, on servers you are using to exchange mail with other mail systems, level 4 switching is not required to provide load balancing and fault tolerance. Instead, load balancing and fault tolerance are provided by publishing multiple MX records in DNS—one for each SMTP server. By giving all MX records the same preference value, incoming mail is automatically distributed across the servers. If one of the servers goes down, the SMTP protocol requires the sending server to try all other MX records before giving up.

Running SMTP services on one or more dedicated servers also insulates the messaging system from SPAM storms. In a "SPAM storm," the messaging system is suddenly besieged by hundreds, if not thousands, of relayed messages and their bounced returns. If the SMTP Agent and its queue server do not reside on the same machine as the client agents or the NMAP Agents responsible for the mail store, it is transparent to users when the system load is heavy.

Hardware-Level Clustering

The message store is the only NetMail component that you cannot clone at the application level. Because only one NMAP Agent is allowed to service a given user context and its associated mailboxes, hardware-level clustering allows the message store to failover to another server in the event of a failure so users can still retrieve their mail.

IMPORTANT: Configuring more than one NMAP server to service the same user context(s) is not allowed and produces unpredictable behavior in the NetMail system.

Hardware-level clustering consists of shared storage and hardware failover. Due to the disk space and hardware requirements, hardware-level clustering is, typically, very expensive.

Hardware

Due to their analog and moving parts, the power supply and disk drives are the most common hardware elements to fail. Consequently, hardware-level clustering usually entails a redundant power supply and a Redundant Array of Independent Disks (RAID).

For NetWare servers running NetMail, Novell recommends RAID level 1 for disk drive redundancy and failover support. Although RAID 1 requires 50% of your disk capacity, it provides the highest level of performance.

RAID 5 does give you the same level of fault tolerance with a smaller percentage of disk space, but it is not as fast as RAID 1. Therefore, because performance is the determining factor in most messaging systems (and because disk space is cheap), RAID 1 is the better choice.

NOTE: For information on configuring NetMail to take advantage of hardware-level clustering, see "Configuring NetMail to Use Hardware Clusters" on page 212.

3 Installing NetMail 3.5

This section guides you through the installation and initial launch of a basic NetMail 3.5 system. It also includes uninstall information.

Section topics include

- "NetMail System Requirements" on page 45
- "Preparing for the Install" on page 46
- "Installing NetMail" on page 48
- "Uninstalling NetMail" on page 50

NetMail System Requirements

The following table outlines the minimum NetMail 3.5 system requirements for Linux* systems. Increase the disk space and memory requirements as per your messaging system configuration.

Requirement	Description
Operating System	RedHat* Linux 7.0 or later (any version of Red Hat Linux supported by eDirectory) with eDirectory 8.6.2 for Linux or higher RedHat Advanced Server 2.1 with eDirectory 8.7 SuSe* Enterprise Edition 8.0 with eDirectory 8.7
Processor	A single processor, server-class PC with a Pentium* II 400 Mhz **NOTE:** NetMail 3.5 for Linux completely supports multiple processors.
Disk Space	20 MB of disk space for installation **NOTE:** Disk space requirements for the NetMail message store varies based on the number of users and the amount of disk space allowed per mailbox. Novell® eDirectory™ requires 3 KB per User object replicated on the server. Therefore, in addition to the standard NetMail disk space requirements, you must calculate an additional 3 KB for every User object in the NMAP Agent's context.
RAM	32 MB of available memory beyond normal Red Hat Linux requirements for a NetMail system of up to 50 simultaneous connections. **NOTE:** Additional connections require additional memory. The POP, IMAP, and Modular Web Agents require additional memory per expected simultaneous connection.

Preparing for the Install

Before installing NetMail 3.5, run through the following checklist:

- Ensure the Directory tree is synchronized and error free. For detailed information, see NDS Health Check procedures (http://www.novell.com/coolsolutions/netmail/features/tips/t_nds_health_check_nm.html) or Keeping eDirectory Healthy.
- Ensure you have Admin rights to the Directory tree where you plan to install NetMail. You must provide the administrator username and password during installation so the installation program can extend the schema.
- If you are running NetMail on NetWare, review Appendix G, "Optimizing a NetWare Server for NetMail," on page 337.
- Decide what you want to name the Messaging Server object. The default is *server_name* Messaging Server.
- Ensure you know the primary Internet domain your NetMail system will service and the IP addresses of primary and secondary DNS servers.
- Check for duplicate port assignments on your server. Conflicts arise if other programs on the server already use those ports.

  NOTE: The NetMail Address Book Agent and eDirectory use the same LDAP port. We recommend that you configure eDirectory to use another LDAP port to avoid a conflict with the NetMail Address Book Agent.

  The following table lists the default NetMail port assignments and their associated agents. It also indicates whether an agent's default port assignment can be reconfigured. To change the port a NetMail agent uses, refer to the agent's configuration options in Appendix H, "NetMail Configuration," on page 343.

Table 4 NetMail Port Assignments

Standard NetMail Port	Novell Nterprise Linux Services	Protocol	Agent	Configurable Port
25	25	SMTP	SMTP Agent	no
80	52080	HTTP	Modular Web Agent	yes
443	52443	HTTPS	Modular Web Agent secure	yes
110	110	POP3	POP Agent	no
995	995	SSL over POP	POP Agent secure	no
143	143	IMAP4	IMAP Agent	no
993	993	SSL over IMAP4	IMAP Agent secure	no
389	52389	LDAP	Address Book Agent	yes
689 UDP	689 UDP	NMAP	NMAP Agent	no
			Connection Manager uses UDP port 689 to receive client IP addresses from the POP and IMAP Agents	
689 TCP	689 TCP	NMAP	NMAP Agent	no

Standard NetMail Port	Novell Nterprise Linux Services	Protocol	Agent	Configurable Port
89	8018	HTTP	WebAdmin Agent	yes
449	8020	HTTPS	WebAdmin Agent	yes
		TLS	NetMail supports TLS on every protocol's native port.	
1026	1026	CAP	Calendar Agent, CAP Agent, ModWeb Calendar Module (they all use CAP?)	no
NA	80	HTTP	Apache Web Server	yes
NA	443	HTTPS	Apache Web Server secure	yes
NA	8008	HTTP	eDir iMonitor	yes
NA	8010	HTTPS	eDir iMonitor secure	yes
NA	389	LDAP	eDir LDAP Server	yes
NA	636	LDAP (SSL)	eDir LDAP Server secure	yes
NA	631	IPP	iPrint IPP Server	yes
NA	443	IPP (SSL)	iPrint IPP Server secure	yes
NA	137	CIFS/SMB	Samba	yes
NA	138	CIFS/SMB	Samba	yes
NA	139	CIFS/SMB	Samba	yes
NA	8080	HTTP	Tomcat	yes
NA	8089	MOD_JK	MOD_JK	yes
524	524	NDAP	eDirectory	no
NA	1229	TED	ZfS	yes

- Before installing NetMail, ensure no one is running WebAdmin.
- If you are upgrading from a previous version, unload NetMail before running the installation.
  - On NetWare, type **`ims u`**
  - On Linux, type **`/etc/init.d/novell-netmail stop`**

  IMPORTANT: All Unload NetMail binaries from previous versions; otherwise, the server abends when you restart NetMail.

Preparing for the Install on Linux Systems

In addition to the preceding preparation steps, you must do the following on Linux systems:

- Stop sendmail on the server where you plan to install NetMail and ensure sendmail is not set to autoload when your server restarts. NetMail 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. (Is this still relevant considering we are using Nsure Audit instead of syslog?)
- Make sure you have access to the install.lin script and its associated rpm files.

  During install, the install.lin script performs the following actions:

  - Verifies that eDirectory for Linux is installed.
  - Installs the Novell Nsure Audit rpm files (NAudit-1.0-1.i386.rpm).
  - Installs the WebAdmin rpm files (WebAdmin-4.0.0-1.i386.rpm).
  - Installs the NetMail rpm files (MDB-1.0.1-1.i386.rpm).
  - Starts the auditext.sh script to create the NetMail Application object.
  - Starts the nimsext.sh script.

Installing NetMail

IMPORTANT: If you are upgrading from NetMail 2.65 or earlier, you must update the location of your SCMS directories after installing NetMail 3.5. For more information, see "SCMSMove" on page 335.

1. Review all the steps in "Preparing for the Install" on page 46 and "Preparing for the Install on Linux Systems" on page 47. In particular:
   - Run ndsstat to make sure NDS is running.
   - If you are upgrading from a previous version, unload NetMail before running the install.
   - Make sure no one is running WebAdmin.
   - Stop sendmail and make sure sendmail is not set to autoload when the server restarts.
2. Log in as root on the host.
3. Type the following command from the setup directory:

   ```
   ./install.lin
   ```
4. When prompted, accept the license agreements for NetMail and Nsure Audit.
5. Type the Directory administrator's login name and password to update the schema.

   This account must have Admin level rights to the root of the tree. If the admin object is not in the same context as the current server, you must type the object's fully distinguished name (for example, .Admin.Accounts.Finance.YourCo).

   If the installation program does not accept your login credentials, type the username in a different format. For example:
   - *user.organizational_unit.organization*
   - *.user.organizational_unit.organization*
   - cn=*user*.ou=*organizational_unit*.o=*organization*
   - .cn=*user*.ou=*organizational_unit*.o=*organization*
6. To extend the Directory schema for NetMail 3.5, select Add Schema Extensions and press Enter.

   Select this option for all first-time NetMail 3.5 installations.

IMPORTANT: Do NOT select this option if NetMail 3.5 has already been installed to another server in your tree.

7 To automatically create the Messaging Server object, the NMAP Agent, and other NetMail Agents in the Internet Services container,

7a Select Configure This Server and press Enter.

Be aware of the following when working in this menu:

- You must tab between the options in this menu. If you press Enter, (verify capitalization) the install program accepts the currently selected options and continues with the install.
- If you enter incorrect information in a particular field, you cannot backspace. To edit a field, tab through all the options until you return to the field you want to edit.
- The space bar (verify capitalization) toggles between field options.

7b Enter the information for the Messaging Server:

- **Official Domain** is the messaging server's Internet domain. All system messages, such as those sent to the Postmaster, use this domain. This is also the default domain for users within the NMAP Agent's supported contexts.

  IMPORTANT: The Official Domain must be a Global Domain; a Hosting Domain is not allowed. For more information on Global and Hosting Domains, see "Global Domains" on page 248 and "Hosting Domains" on page 250.

  You must register the Official Domain Name in DNS before the messaging system can send and receive mail via the Internet.

- **Primary and Secondary DNS Server** is the IP address of a primary and secondary (optional) DNS server that resolves host names into IP addresses for your NetMail system.

7c Select which agents you want to create. You can create the following agents from the install program:

SMTP Agent	POP Agent
IMAP Agent	ModWeb Agent
Forward/AutoReply Agent	Address Book Agent (LDAP)
Calendar Agent	Proxy Agent
AntiSpam Agent	

NOTE: You cannot create the List, Rule, AntiVirus, CAP, and Connection Manager agents until after NetMail is installed.

For detailed information on each agent's configuration options, see "NetMail Agent Configuration Options" on page 359.

8 When finished, select Exit NIMSEXT and press Enter.

9 After install, NetMail automatically launches on Linux systems.

For instructions on manually starting or stopping the system, see "Starting and Stopping NetMail on Linux" on page 316.

When the installation is complete, the Directory tree includes the following objects:

- The Internet Services Container with the following:

- The Mailing Lists container
- The Parent Objects container
- The Templates container (Check to see if we install WebAccess and WebMail by default)
- Any NetMail objects created using the Configure This Server option

- The Logging Services container with the following:
  - The Application container with Application objects for NetMail and the Naudit, eDirectory, and NetWare instrumentations
  - The Channel container with a File Channel object
  - The Notification container

Uninstalling NetMail

To uninstall NetMail:

1. Run the NIMSEXT utility to remove the NetMail schema.

   For more information about the NIMSEXT utility, see "NIMSEXT" on page 332.

2. Delete the NetMail binary, mailbox, and message queue directories.

   For a complete listing of the Netmail directories for each platform, see Appendix I, "Quick Reference Matrix," on page 403.

4 WebAdmin

NetMail™ is managed using WebAdmin. WebAdmin is a highly flexible, browser-based administrative tool. Because it is browser-based, WebAdmin is platform independent. You can manage your system on virtually any operating system for which there is an Internet-standard browser.

WebAdmin runs on most current browser versions including Internet Explorer 5.x and higher, Netscape* 6.x, Mozilla* 1.3, and Opera* 7.x. Basically, WebAdmin runs on any browser that provides good Javascript* support.

NOTE: WebAdmin does NOT run on Netscape 4.x.

This section walks you through the WebAdmin interface and shows you how to perform basic system functions.

- "Webadmin Interface" on page 51
- "Installing WebAdmin" on page 54
- "Opening WebAdmin" on page 54
- "Performing Basic Administrative Functions in WebAdmin" on page 56

Webadmin Interface

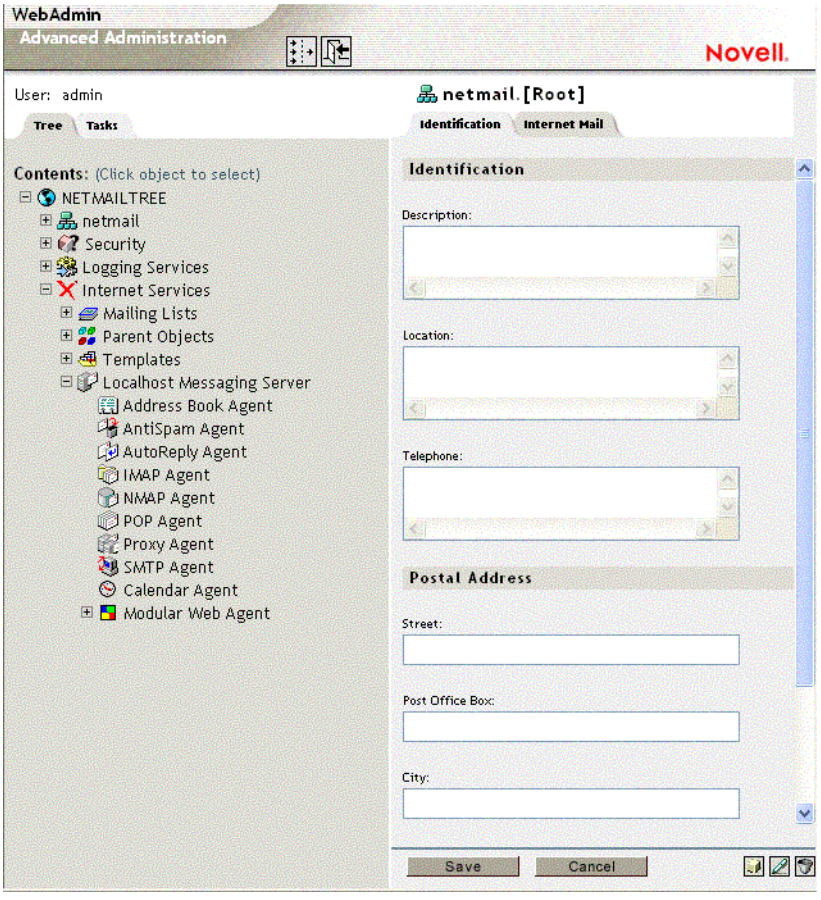
WebAdmin provides both a traditional, tree-oriented view and a task-based view.

IMPORTANT: Do not use the browser's Back and Forward buttons while using WebAdmin. Because WebAdmin is a Web-based application, it is important to navigate through the interface using the buttons inside the application, not the buttons on the browser's toolbar.

Tree View

In the Tree view, a full, graphical representation of the tree displays in the left frame while the Properties menus appear in the right frame. If you are using Internet Explorer 6.0, WebAdmin also gives you a right-click quick menu.

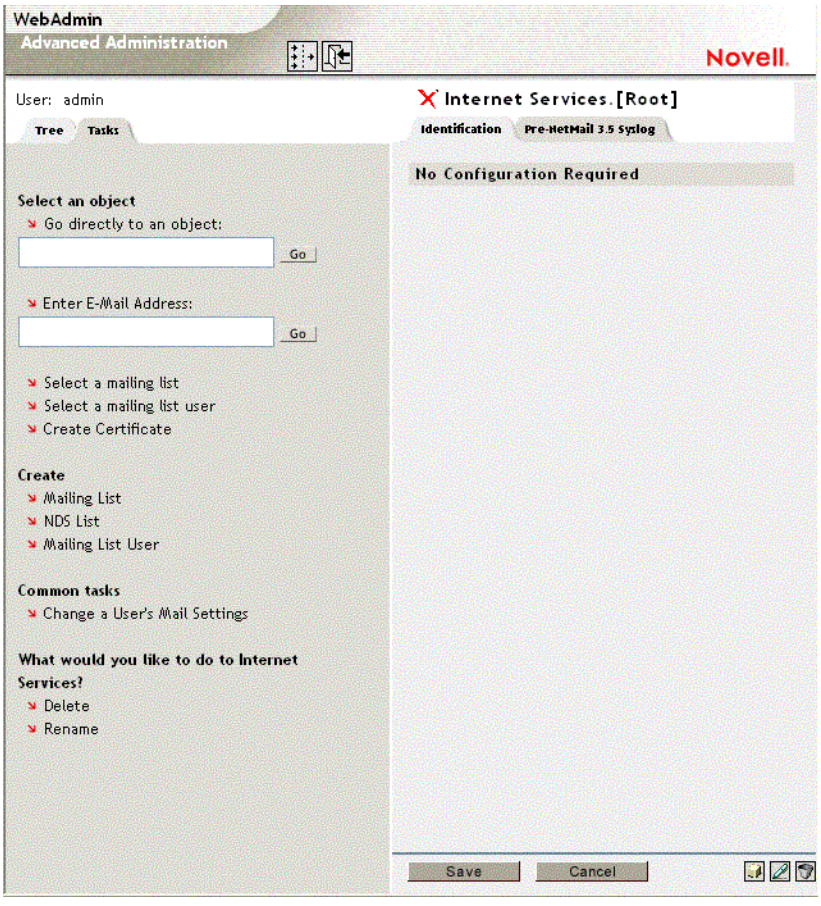
Description: WebAdmin Tree View



Task View

The Tasks view provides several tools to help you quickly locate specific objects and perform common administrative functions.

Description: WebAdmin Task View



To select a specific object, you can type the object's fully distinguished name or, in the case of User objects, you can type the user's Internet e-mail address. Additionally, you can select a specific mailing list or mailing list user.

The other tasks in this view guide you through common administrative tasks such as creating Mailing Lists or changing a User's mail settings. The following table provides a brief description of each task.

Table 5 Common Administrative Tasks

Task	Description
Create Mailing List	Creates a Mailing List object in the Mailing Lists container under Internet Services. For more information, see "Mailing Lists" on page 273.
Create NDS List	Creates an NDS Mailing List object in the Mailing Lists container under Internet Services. For more information, see "NDS Mailing Lists" on page 271.
Create Mailing List User	Allows you to create a Mailing List User for a specific Mailing List. For more information, see "List User Objects" on page 277.
Create Certificate	Generates a Certificate Signing Request (CSR), a self-signed certificate, or a root certificate. For more information, see xx.

Task	Description
Change a User's Mail Settings	Allows you to change a specific mail setting for a given user. The available mail settings are as follows: ◆ Reply To Address ◆ Privacy Settings ◆ Forwarding Settings ◆ Auto Reply Settings ◆ Time Zone ◆ Quota ◆ Disable Email Access For a description of these mail settings, see Table 5, "User Objects," on page 394.

In addition to these basic tasks, WebAdmin provides a dynamic list of tasks based on the currently selected object. In most cases, you can choose a task to rename or delete the current object. However, in some instances, there are tasks that change specific object properties. For example, if you select a Mailing List object, WebAdmin provides a list of tasks that allow you to change the Mailing List abstract, description, moderators, access settings, and so forth.

NOTE: For an explanation of any object property, see Appendix H, "NetMail Configuration," on page 343.

Installing WebAdmin

WebAdmin is automatically installed with NetMail 3.5, so no additional installation is required.

During installation, the WebAdmin program file is installed to the following directories:

Table 6 WebAdmin Installation Directory Structure

Operating System	Directory
NetWare®	sys:\system\webadmin.nlm **NOTE:** The remaining files are in sys:system\webadmin\.
Windows	\program files\novell\webadmin\webadmin.exe
Linux	/opt/novell/bin/webadmin **NOTE:** The remaining files are in /opt/novell/WebAdmin/.

Opening WebAdmin

IMPORTANT: WebAdmin uses popup windows; consequently, WebAdmin cannot work if you are using an HTTP proxy to filter popup ads.

To open WebAdmin:

1 Load the WebAdmin program file.

1a On a NetWare server, type `load webadmin` at the console prompt.

1b On a Windows server, the WebAdmin service loads automatically.

1c On a Linux server, type **`/opt/novell/bin/webadmin`**.

2 In your Web browser, type the URL or host name of the server running WebAdmin, including the port number. For example:

```
http://127.5.4.1:89
```

```
https://127.5.4.1:449
```

NOTE: By default, WebAdmin uses port 89 for HTTP and port 449 for HTTPS connections; on Novell® Nterprise™ Linux Services, WebAdmin uses port 8018 for HTTP and 8020 for HTTPS connections. You can change WebAdmin's default port assignments using the -p and -s switches. For more information, see "WebAdmin Startup Commands" on page 55. For information on WebAdmin and HTTPS, see "Securing Your WebAdmin Connection" on page 55.

3 When prompted, type your User object's distinguished name (for example, `admin.users`)and password to bring up the WebAdmin console.

WebAdmin Startup Commands

Use the following switches with the **`webadmin`** command:

Check to see if there are more switches.

Table 7 Switches for use with webadmin command

Switch	Description
-h or -?	Lists the WebAdmin switches and their variables.
-d	Turns on debugging; this is primarily used by Novell® Technical Services℠.
-p:*port*	Changes WebAdmin's HTTP port assignment. The default port assignment is 89. On Novell Nterprise Linux Services, the default port assignment is 8018. **IMPORTANT:** Do not attempt to secure access to WebAdmin by reassigning its port assignment. While changing the port assignment obscures the connection, it does not provide a high level of security.
-s:*SSL_port*	Configures WebAdmin to accept secure HTTP connections (HTTPS) at the designated port. The default port assignment is 449. On Novell Nterprise Linux Services, the default port assignment is 8020. For information on WebAdmin and HTTPS, see "Securing Your WebAdmin Connection" on page 55.

Securing Your WebAdmin Connection

WebAdmin includes its own built-in certificate to secure your WebAdmin connection. This certificate allows you to encrypt your connection to WebAdmin; however, it is not necessarily "secure" because the same certificate is distributed with every copy of WebAdmin.

If you want to truly secure your connection to WebAdmin, you must obtain a server certificate from a Certificate Authority (CA). A 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™.

To select a CA, check your browser 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 browsers.

After you obtain your certificate, you must put the certificate and private key files (*.pem) in one of the following directories on the WebAdmin server:

Table 8 WebAdmin Certificate Directory for Each Operating System

operating System	WebAdmin Certificate Directory
NetWare	sys:\system\webadmin\
Windows	\program files\novell\webadmin\
Linux	/opt/novell/WebAdmin/

With your certificate and private key files in the correct directory, you can connect to WebAdmin over a secure connection. Simply type the URL or host name of the server running WebAdmin and designate a connection at port 449 or, on Novell Nterprise Linux Services, port 8020. For example,

```
https://127.5.4.1:449
```

NOTE: You can change the default port for secure connections using the -s startup switch. For more information on WebAdmin startup switches, see "WebAdmin Startup Commands" on page 55.

Performing Basic Administrative Functions in WebAdmin

This section reviews how to perform the following administrative functions:

- Creating Objects in WebAdmin
- Renaming Objects in WebAdmin
- Deleting Objects in WebAdmin
- Modifying Object Attributes in WebAdmin

IMPORTANT: Do not use the browser's Back and Forward buttons while using WebAdmin. Because WebAdmin is a Web-based application, it is important to navigate through the interface using the buttons inside the application, not the buttons on the browser's toolbar.

Creating Objects in WebAdmin

To create an object in WebAdmin:

1. In the Tree view, select the container where you want to create the object.
2. Click the Create icon  .

   HINT: In Internet Explorer 6.0, you can right-click the container where you want to create the object and select Create from the quick menu.
3. In the Create menu, select the type of object you would like to create.
4. Type the object name and any other required information.
5. When finished, click Save.

IMPORTANT: When you create a NetMail Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

In addition to creating objects from the Tree view, the Task view provides tasks that allow you to to create the following objects:

- Mailing Lists (For more information, see "Mailing Lists" on page 273.)
- NDS Lists (For more information, see "NDS Mailing Lists" on page 271.)
- Mailing List Users (For more information, see "List User Objects" on page 277.)
- Certificates (For more information, see xx.)

Renaming Objects in WebAdmin

To rename an object in WebAdmin:

1. In the tree view, select the object you want to rename.
2. Click the Rename icon  .

   HINT: In Internet Explorer 6.0, you can right-click the object and select Rename from the quick menu or you can select the Rename task from the Task view.
3. Type the object's new name.

   IMPORTANT: Do not include the context with the new object name.
4. When finished, click Save.

Deleting Objects in WebAdmin

To delete an object in WebAdmin:

1. In the tree view, select the object you want to delete.
2. Click the Delete icon  .

   HINT: In Internet Explorer 6.0, you can right-click the object and select Delete from the quick menu. You can also select the Delete task from the Task view.
3. Click OK to delete the object.

Modifying Object Attributes in WebAdmin

To define object attributes in WebAdmin:

1. Select the object.
   - In the Tree view, select the object in the left frame.
   - To go directly to an object, type the object's fully distinguished name in the Task view's Go Directly to an Object field and click Go.
   - To go directly to a specific User object, type the user's Internet e-mail address in the Task view's E-Mail Address field and click Go.
2. Modify the object's attributes in the right frame of the tree view.
3. When finished, click Save.

   IMPORTANT: If you modify attributes in multiple tabs, you must click Save in each screen to apply your changes.

   In some cases, you must restart the messaging server to implement changes to an agent's configuration. Appendix E, "Implementing Administrative Changes," on page 303 documents what is required to implement administrative changes for each property. These requirements are also noted in each agent's configuration section. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

To modify a specific user's mail settings:

1. In the Task view, click Change a User's Mail Settings.
2. Select the specific property you want to modify.
3. Type the user's Internet e-mail address.
4. Modify the setting.
5. Click Finish to apply the setting.

5 Setting Up Your Messaging Server and NMAP Agent

The messaging server and NMAP Agent are NetMail's core components. They impact every other component in the messaging system. Consequently, creating and configuring the messaging server and NMAP Agent are critical in building a functional messaging system.

This section helps you successfully create and configure your system's messaging server and NMAP Agent.

Section topics include

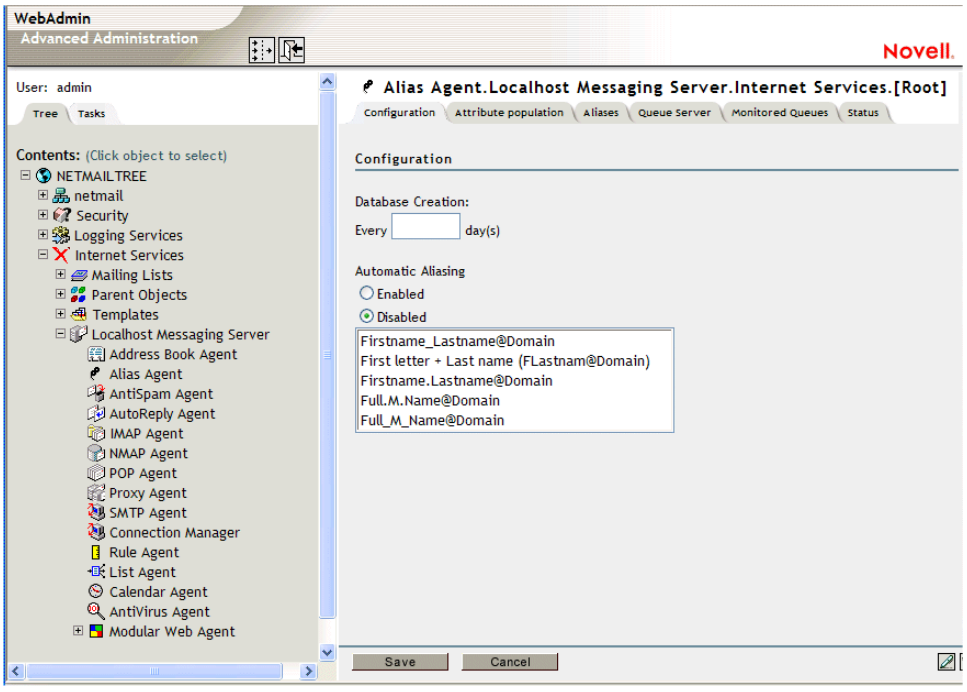
- "Messaging Server" on page 59
  - "Creating the Messaging Server" on page 60
  - "Configuring the Messaging Server" on page 63
- "NMAP Agent" on page 67
  - "Creating the NMAP Agent" on page 68
  - "Configuring the NMAP Agent" on page 68

Messaging Server

Description: Messaging Server icon

A *messaging server* is any server on the network that hosts one or more NetMail agents. In eDirectory™, the messaging server is represented as a Container object with server attributes: it sets the messaging server properties and it "contains" all NetMail agents running on that server.

Description: Messaging Server and Agents within WebAdmin



Creating the Messaging Server

In creating Messaging Server objects, there are three primary considerations:

- Distributed or Standalone?
- Where to Create the Messaging Server Object
- How to Create the Messaging Server Object

Each of these issues is discussed in the following sections.

Distributed or Standalone?

The first issue to consider before creating your Messaging Server object is whether the messaging server is going to in distributed or standalone mode.

By default, messaging servers are created in distributed mode; that is, they look for other Messaging Server objects in the Internet Services container. This enables messaging system functions to be distributed over several servers.

Standalone messaging servers do not search the Directory tree for Internet Services and its associated messaging servers. Instead, they act as independent messaging systems, exclusively providing all NetMail services to the users within their assigned contexts.

To configure a standalone messaging server, you must mark the **Distributed Processing Disabled** option in the messaging server's configuration menu. This prevents the messaging server from looking for other Messaging Server objects in the Internet Services container.

NOTE: For an overview of standalone and distributed messaging servers, see "Messaging Server" on page 2. For help in determining whether distributed or standalone messaging servers best suit your messaging system environment, see "Selecting Your NetMail System Configuration" on page 28.

Where to Create the Messaging Server

Associated with the question of whether to operate a messaging server in distributed or standalone mode is the issue of where to create the Messaging Server object.

Typically, messaging servers are created in the Internet Services container because most messaging systems function in distributed mode and distributed messaging servers look for other Messaging Server objects in the Internet Services container.

In some instances, however, messaging systems require standalone configurations. Messaging Server objects located outside the Internet Services container are not recognized by other messaging servers. Consequently, standalone messaging servers are usually created outside Internet Services.

NOTE: By default, all messaging servers search the Directory tree for other messaging servers in Internet Services, even those created outside the Internet Services container. Therefore, you must mark the Distributed Processing Disabled option in the messaging server's configuration menu to define a standalone messaging server, even if it is created outside Internet Services.

Creating Distributed Messaging Servers Outside Internet Services

In some situations, you might want to create a Messaging Server object outside the Internet Services container and have it continue to function in distributed mode. For example, to easily delegate system administration, you can create messaging servers in the same containers as the users they service and simply grant administrative rights on a container basis.

Messaging servers created outside the Internet Services container can continue to operate in distributed mode if you create Alias objects for them within Internet Services. Alias objects enable distributed messaging servers to locate and interact with messaging servers outside the Internet Services container in the same way they interact with messaging servers inside the Internet Services container.

NOTE: You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Internet Services container.

How to Create the Messaging Server

NetMail 3.5 gives administrators the option of creating the Messaging Server object during installation or creating it after installation using WebAdmin.

How you choose to create the Messaging Server object depends, in part, on where you want to create the messaging server. Creating the messaging server during installation automatically creates the object in the Internet Services container. If you want to create the messaging server outside of the Internet Services container, you must create the object after installation using WebAdmin.

The basic processes of creating the Messaging Server object during or after installation are outlined in the following sections.

Creating the Messaging Server During Installation

In creating the Messaging Server object, the installation program prompts you for the following information:

Table 9 **Creating the Messaging Server During Installation**

Option	Function
Server Name	A unique name for the Messaging Server object in eDirectory.
Official Domain Name	The Internet domain serviced by the current messaging server (such as abc.com or 123.net). All system messages, such as those sent to the Postmaster, use this domain. Additionally, if the messaging server is running the NMAP Agent, the Official Domain Name is the default domain for users within the NMAP Agent's context. **IMPORTANT:** For the Official Domain, a Global Domain is required; a Hosting Domain is not allowed. For more information on Global and Hosting Domains, see "Global Domains" on page 248 and "Hosting Domains" on page 250. You must register the Official Domain Name in DNS before the messaging system can send and receive mail via the Internet. NetMail can share an Internet domain with other messaging systems. NetMail can 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 "Domain Sharing" on page 251.
Primary and Secondary DNS Servers	The IP address of a primary and secondary (optional) DNS server that resolves host names into IP addresses for your NetMail system.

The installation program automatically creates a Messaging Server object with an NMAP Agent in the Internet Services container.

NOTE: For more information on the installation process, see Chapter 3, "Installing NetMail 3.5," on page 45.

Creating the Messaging Server after Installation

After installing NetMail 3.5, you can create Messaging Server objects using WebAdmin. To create the messaging server object, select the container in which you want to create the messaging server and choose Novell® NetMail from the Create menu.

In creating the Messaging Server object, you are prompted for the following information:

Table 10 **Creating the Messaging Server After Installation**

Option	Function
Server Name	A unique name for the Messaging Server object in eDirectory.
NetWare® Host	The distinguished name of the messaging server's NCP Server object. The host is selected when creating the Messaging Server object.

Option	Function
PostMaster	The user assigned to manage the messaging server. This user can also receive copies of bounced messages. (See the CC PostMaster property in Table 4, “Configuring the NMAP Agent,” on page 68.) Click the browse button to select the PostMaster in the Directory tree. **IMPORTANT:** The PostMaster must belong to a Global Domain. You cannot designate Hosting Domain users as the messaging server PostMaster. For more information on Global and Hosting Domains, see “Global Domains” on page 248 and “Hosting Domains” on page 250. **IMPORTANT:** Do NOT delete the User object designated as the messaging server postmaster. You must reassign the PostMaster before deleting an existing PostMaster User object. Deleting the Postmaster’s User object changes Messaging Server object to type “Unknown.” Consequently, the Messaging Server object appears with a “?” in eDirectory. To reset Messaging Server object type, you must run the IMSPMFIX utility. You can download this utility at http://www.novell.com/coolsolutions/netmail/features/a_product_updates_nm.html.
Official Domain Name	The Internet domain serviced by the current messaging server (such as abc.com or 123.net). All system messages, such as those sent to the Postmaster, use this domain. Additionally, if the messaging server is running the NMAP Agent, the Official Domain Name is the default domain for users within the NMAP Agent’s context. **IMPORTANT:** For the Official Domain, a Global Domain is required; a Hosting Domain is not allowed. For more information on Global and Hosting Domains, see “Global Domains” on page 248 and “Hosting Domains” on page 250. You must register the Official Domain Name in DNS before the messaging system can send and receive mail via the Internet. NetMail can share an Internet domain with other messaging systems. NetMail can 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 “Domain Sharing” on page 251.

Configuring the Messaging Server

From the Messaging Server’s Details menu, you can configure the following options:

Table 11 Configuring the Messaging Server

Option		Function
Identification		
	NetWare Host	The fully distinguished name of the messaging server’s NCP Server object. The host is selected when creating the Messaging Server object. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)

Option		Function
	PostMaster	The user assigned to manage the messaging server. This user can also receive copies of bounced messages.(See the CC PostMaster property in Table 4, “Configuring the NMAP Agent,” on page 68.) Click the browse button to select the PostMaster in the Directory tree. **IMPORTANT:** The PostMaster must belong to a Global Domain. You cannot designate Hosting Domain users as the messaging server PostMaster. For more information on Global and Hosting Domains, see “Global Domains” on page 248 and “Hosting Domains” on page 250. **IMPORTANT:** Do NOT delete the User object designated as the messaging server postmaster. You must reassign the PostMaster before deleting an existing PostMaster User object. Deleting the Postmaster’s User object changes Messaging Server object to type “Unknown.” Consequently, the Messaging Server object appears with a “?” in eDirectory. To reset Messaging Server object type, you must run the IMSPMFIX utility. You can download this utility at http://www.novell.com/coolsolutions/netmail/features/a_product_updates_nm.html. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)
	Official Domain	The Internet domain serviced by the current messaging server (such as abc.com or 123.net). All system messages, such as those sent to the PostMaster, use this domain. Additionally, if the messaging server is running the NMAP Agent, the Official Domain Name is the default domain for users within the NMAP Agent’s context. **IMPORTANT:** For the Official Domain, a Global Domain is required; a Hosting Domain is not allowed. For more information on Global and Hosting Domains, see “Global Domains” on page 248 and “Hosting Domains” on page 250. You must register the Official Domain Name in DNS before the messaging system can send and receive mail via the Internet. NetMail can share an Internet domain with other messaging systems. NetMail can 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 “Domain Sharing” on page 251. Changes to this property are effective within 5 minutes.
	Temp Directory	The volume and, optionally, the directory where NetMail agents write temporary files. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)

Option		Function
	DBF Directory	The volume and, optionally, the directory where the NetMail alias database, address book, and queue client files are stored. The queue client files track every NetMail agent that has registered with NMAP; if the NMAP server goes down, the NMAP Agent can re-establish its client connections. Queue client files are most pertinent in distributed environments where NMAP clients can reside on different messaging servers than the NMAP Agent. the NMAP Agent. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
	Resolver(s)	The IP address of one or more DNS servers that resolve host names into IP addresses. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
	Distributed Processing Disabled	Disables the messaging server's ability to interact with other messaging servers via NMAP. Marking this option creates a standalone messaging server; that is, the messaging server no longer searches the Directory tree for Internet Services and its associated messaging servers. By default, all messaging servers search the Directory tree for other messaging servers in Internet Services, even those created outside the Internet Services container. Therefore, you must mark this option to create a standalone messaging server, even if it is created outside Internet Services. **NOTE:** For help in determining whether distributed or standalone messaging servers best suit your messaging system environment, see "Selecting Your NetMail System Configuration" on page 28. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
	Conn. Mgr.	The fully distinguished name of the server running the Connection Manager. You must have a Connection Manager running in your messaging system to configure this option. **IMPORTANT:** To have a comprehensive record of all authenticated users, you can only have one Connection Manager per messaging system. Connection Manager tracks the IP addresses of authenticated users. If this field is completed, any agent running on the current messaging server can query the Connection Manager Agent to verify that a user has authenticated with the system. For example, the SMTP Agent utilizes the Connection Manager Agent for SMTP-after-POP authentication. Changes to this property are effective within 5 minutes. **NOTE:** For more information, see "SMTP-after-POP" on page 232 or "Connection Manager" on page 243.

Option		Function
Security		NetMail supports Secure Socket Layer (SSL) security. SSL secures information passed between mail clients and the messaging server through public key encryption. SSL does *not* secure messages leaving your mail system nor does it secure message content. However, you can use TLS to encrypt server-to-server Internet communications as long as both sides of the transaction support TLS. **NOTE:** To secure message content, users must have an X.509 certificate. To enable SSL and TLS, you must first have a server certificate installed on your messaging server. For information on setting up your server certificate, see "Setting Up TLS and SSL" on page 231.
	Enable SSL and TLS	Marking the Enable SSL and TLS option allows mail clients to connect to the messaging server over an SSL or TLS connection. It also enables the messaging server to automatically switch into encrypted mode when communicating with other TLS-enabled mail servers. You must have a server certificate installed on your messaging server before you can enable this option. See "Setting Up TLS and SSL" on page 231 for more information. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
	Server Managers	Users who are given rights to access NetMail administrative utilities like RMBOX. The designated user must authenticate to these utilities by providing his or her NetMail username and password. Changes to the Server Managers property are immediately implemented **NOTE:** For more information, see "RMBOX" on page 334.
	Statistics	The Statistics page is only available on NetWare servers. It provides up-to-date resource and performance statistics for a NetWare server—essentially the same statistical information as the MAILCON utility. This page is useful to those 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 are 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 Modular Web Agents ◆ The total number of server connections; that is, the number of SMTP, WebAccess, 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 NetWare and Windows servers, launch MAILCON. On Linux systems, run NMAIL. For more information on these commands and utilities, see Appendix F, "NetMail Commands and Utilities," on page 315.

Option		Function
SNMP Configuration		NetMail supports SNMP (Simple Network Management Protocol), allowing you to use management tools such as HP OpenView* or Novell ManageWise® to detect problems, optimize server performance, and obtain long-term trending information. Provides organization, location, contact, and name information for the messaging server to pass to SNMP applications that request information about the messaging server. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
	Organization	
	Location	
	Contact	
	Name	
Status		
	Status	Displays the IP address of the messaging server and its current status. The messaging server status is either "Running" or "Shut Down." By default, the messaging server is enabled. To disable the messaging server, 1. Mark Disable Server. 2. Click OK. Marking Disable Server prevents the messaging server from launching at server startup. However, to immediately disable the messaging server, you must manually unload IMS.NLM or restart the server. For more information on unloading the messaging server, see "NetMail Startup Commands" on page 316. After the messaging server is disabled, the server does not launch IMS.NLM again until you deselect the Disable Server option and restart the server.
	Force Server IP Address To	The messaging server's IP address. NetMail agents running on other messaging servers use this IP address to communicate with an NMAP Agent running on the current messaging server. This option is useful for clustering applications, such as Novell Clustering Services (NCS), that use secondary IP addresses.
	Force agent bind to specified address only	By default, NMAP binds to all IP addresses found on a machine. Marking this option forces NMAP to only bind to the above listed IP address.

NMAP Agent

Description: IMAP Agent icon

The NMAP Agent is responsible for message processing and delivery. It handles everything that happens from the time a message enters the message queue to when it is delivered to the user's mailbox or passed off for delivery via the Internet. Indeed, it is the only agent that has direct access to the message store. Consequently, every messaging system requires at least one NMAP Agent and every user within the messaging system must be included in one of the NMAP Agent's contexts.

Creating the NMAP Agent

To create the NMAP Agent, select the messaging server on which you want to create the NMAP Agent and choose NMAP Message Store from the Create menu.

In creating the NMAP Agent object, you are prompted for the following information.

Table 3 Information Needed When Creating an NMAP Agent Object

Option	Function
Base Directory for Message Store	The volume and, optionally, the directory where users' mailboxes are located. On a NetWare server, the message store's default location is sys:\NOVONYX\MAIL. On a Windows server, the default message store directory is \Program Files\novell\netmail\mail. On a Linux server, the default location is the /usr/nims directory. For a more complete explanation, see the Message Store property in Table 4, "Configuring the NMAP Agent," on page 68.
Context	The eDirectory context serviced by the current NMAP Agent. When creating the NMAP Agent, you can only select one context. However, when configuring the NMAP Agent, you can add multiple user contexts. For a more complete explanation, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

After you create the NMAP Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the NMAP Agent

From the NMAP Agent's Details menu, you can configure the following options:

This table also has some interface changes and new undocumented UI items. Status has really changed.

Table 4 Configuring the NMAP Agent

Option	Function
Parameters	
Storage Paths	**IMPORTANT:** You must restart NMAPD to effect any changes in these properties. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option		Function
	Message Store	The volume and, optionally, the directory where users' mailboxes are located. On a NetWare server, the message store's default location is sys:\NOVONYX\MAIL. On a Windows server, the default message store directory is \Program Files\novell\netmail\mail. On a Linux server, the default location is the /usr/nims directory. For detailed information about the message store directory structure, see "Message Store Directory Structure" on page 19. **IMPORTANT:** Because NetWare requires free space on the sys: volume, 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, 1. Stop the NMAP Agent. 2. Move the existing message store directory to its new location. 3. Change the location specified in the NMAP Agent's Message Store field. 4. Restart the NMAP Agent. (See "Loading and Unloading NetMail Agents" on page 317.) **IMPORTANT:** It is best to change the message store volume before you put your NetMail system into production. In addition to the primary message store on the messaging server, you can define message store directories for Container and Parent objects. For more information, see "Creating Separate Message Stores for Each Domain" on page 260.
	Spool Directory	The volume and, optionally, the directory where you want the message queue to reside. For detailed information about the Spool directory structure and how the message queue works, see "Message Processing" on page 19.
	Minimum Space	The minimum amount of free space you want to maintain on the volume hosting the message queue. The default is 2048 KB. If the server reaches the Minimum Space quota, the messaging server bounces all incoming messages, stops system logging, and sends an SNMP trap. If your mail directories are on the sys: volume, you can use this option to maintain the free space required by NetWare.
	SCMS Directory	The volume and, optionally, the directory where you want the Single Copy Message Store (SCMS) directory to reside. For detailed information about the SCMS directory structure and how it works, see "Single Copy Message Store" on page 20.
Queue Parameters		

Option		Function
	Retry Interval	The number of minutes the NMAP Agent waits before trying to resend any e-mail message. The default is 30 minutes. NetMail never queues messages unless there is a problem. Under normal conditions, the NMAP Agent immediately tries to send messages after they are processed in the queue. If, for some reason, the message is not sent, it remains in the queue for the number of minutes specified in the Retry Interval before NMAP tries to resend the message. For example, if you send a message to a company whose mail server is down, the messaging server keeps trying to send the message at the designated intervals. Changes to this property are effective within 5 minutes.
	Retry Timeout	The number of days the NMAP Agent keeps trying to send any e-mail message before removing the message from the queue. The default is five days. The NMAP Agent attempts to bounce undeliverable messages before removing them. **IMPORTANT:** You must restart NMAPD to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option		Function
Options		
	Bounced Message Control	A UBE control feature that sets a threshold for the number of bounced messages NMAP can process within a set number of seconds. If the number of bounced messages exceeds the defined threshold, the messages are deleted, not processed. It is a common practice for spammers to falsify the From: field in their message so the resulting bounced messages go to a mail server other than their own. Unfortunately, the server that actually owns the domain specified in the From: field is inundated with thousands of bounced messages in a short period of time. The Bounced Message Control feature enables you to keep your NetMail system from wasting system resources during such attacks. Changes to this property are effective within 5 minutes.
	CC Postmaster	Mark this option to send the Postmaster a copy of bounced messages.
	Limit Bounces To	Select this option to turn on Bounced Message Control. ◆ **Interval:** The time frame threshold (in seconds). ◆ **Entries:** The number of bounced messages NMAP can process during the *Interval* time frame. If the number of bounced messaged exceed the *Entries* threshold within the *Interval* time frame, NMAP deletes the messages.
	Forward Local Undeliverable Messages	The host name or IP address of a server designated to receive messages that are addressed to the messaging system's domain but are undeliverable within the local NetMail 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 e-mail address. Changes to this property are effective within 5 minutes. When the NMAP Agent determines that a message recipient is within its Internet domain but cannot find the user in eDirectory, the NMAP Agent modifies the domain portion of the address with the value placed in this field and re-queues the message. Commonly, use this feature in WAN environments with standalone messaging servers in remote offices. For detailed information on this configuration, see "Multiple Messaging Server WAN" on page 36. This option also enables NetMail to share a domain name with another e-mail system such as Novell GroupWise®, Lotus Notes*, or Microsoft* Exchange. When this option is configured, the NMAP Agent forwards messages that belong to the domain but are not addressed to users within the NetMail messaging system. For more information on domain sharing, see "Domain Sharing" on page 251.

Option	Function
Remote Queue Restrictions	Regulates when remote messages are passed to the SMTP Agent for delivery across the Internet. If Do not process remote queue is selected, NMAP holds remote messages in queue 7 until the designated time frames. Only then does it notify the SMTP Agent to pick up the messages. In the Weekdays field, specify a time span (using the 24-hour clock) when you do not want the NMAP Agent to process outgoing messages Monday through Friday. In the Weekends field, do the same for Saturday and Sunday. This feature is for countries where users must pay a per use line fee. Using this option, you can restrict remote message delivery to non-peak hours. **IMPORTANT:** You must restart NMAPD to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Context	The eDirectory contexts serviced by the current NMAP Agent. The original context was defined when creating the NMAP Agent. Add other user contexts from the Context page. Because NMAP contexts are not inherited, add every container or sub-container serviced by an NMAP Agent to that agent's context list. Messaging services are automatically provided to every user in the NMAP Agent's assigned contexts. User mailboxes are created in the local message store directory the first time users log in or receive messages. **IMPORTANT:** Do not add the same context to multiple NMAP Agents.This produces unpredictable behavior in NetMail systems. In previous NetMail versions, the messaging server's context list was not updated in memory. Consequently, if you added or removed contexts in the NMAP Agent configuration, the changes did not take effect until the messaging server was restarted. In NetMail 3.5, however, the messaging server's context list is updated in memory; therefore, it is no longer necessary to restart the messaging server. The Messaging Server's Context List NMAP contexts are tracked by the messaging server. When it starts, the messaging server generates a list of NMAP contexts and holds it in server memory. In distributed environments, the context list includes the assigned contexts for every NMAP Agent in the Internet Services container. On standalone messaging servers, this list only includes the local NMAP Agent's assigned contexts. NetMail agents reference the messaging server's context list in providing user-related services. If a user is not included in the list, the agent's services are denied. For example, users cannot establish a POP or IMAP connection to the messaging system unless they are in the context list. System Requirements eDirectory requires a minimum of 3 KB per User object replicated on the server. Therefore, in addition to the standard NetMail disk space requirements, you must calculate at least an additional 3 KB for every User object in the NMAP Agent's context. Additionally, the NMAP Agent requires local access to all User objects within its assigned contexts.

Option		Function
Mailbox Quota		The system administrator can define mailbox quotas for specific users or for all users serviced by the current NMAP Agent. Messages, folders, and calendar items count against the mailbox quota. **IMPORTANT:** You must restart NMAPD to effect any changes in these properties. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
	Per User Mailbox Quotas	Mark this option to require individual user quotas. User quotas are set in the NetMail Configuration page of the User object. For further information on User object configuration, see Table 5, "User Objects," on page 394.
	System-Wide Mailbox Quotas	To set the same quota for all mailboxes on the current messaging server, mark this option and type the maximum mailbox size in the Kbyte field. If you select both Per User and System-Wide Mailbox Quotas, you can set quotas at both levels. While the system-wide quota serves as the default quota for all users in the NMAP Agent's assigned contexts, quotas defined in the User object take precedence. For example, you can set a default, system-wide mailbox quota but still allocate more disk space to specific users such as the messaging server postmaster, system administrators, or VIPs using User object mailbox quotas. **NOTE:** You can also define mailbox quotas at the Parent object level. For more information on Parent object mailbox quotas, see the Mailbox Quota property in Table 3, "Configuring Parent Objects," on page 262.
	Quota Return Message	An optional message that is returned to the sender when the recipient has exceeded his or her mailbox quota.The message notifies the sender that the recipient has exceeded the allotted mailbox quota and cannot receive additional messages. **NOTE:** When users are within 10% of their mailbox quota, they receive a system message notifying them that their mailbox is almost full. The message advises them to delete some of the messages and warns that when their mailbox is full, all inbound messages are returned to the sender.
Single Copy Message Store		The Single Copy Message Store (SCMS) feature allows NMAP to store e-mail messages sent to multiple recipients in a shared location on the messaging server. By default, messages sent to five or more users and exceeding 5 KB are stored in the shared message directory. To store a message in the SCMS directory, it must exceed both thresholds. When a message exceeds the specified thresholds, NMAP places a single copy of the message and its attachments in the shared message directory. A pointer is placed in the recipients' mailboxes, directing NMAP to the complete message in the Single-Copy Message Store (SCMS) directory. When the last user downloads or deletes the message, it is deleted from the shared directory. The SCMS feature conserves server disk space. Without SCMS, long messages and large attachments are sent to every recipient's mailbox, rapidly consuming large amounts of server disk space. Changes to this property are effective within 5 minutes. For more information on the SCMS directory, see "Single Copy Message Store" on page 20.

Option		Function
	Minimum Number of Recipients	The SCMS threshold for a message's number of recipients. If the number of message recipients is equal to or more than the designated number of recipients and it exceeds the Minimum Message Size threshold, it is stored in the SCMS directory.
Trusted Hosts		When NetMail agents need to access the message store or message queue, they create an IP connection to the associated NMAP Server and request the information they need. By default, the NMAP Agent requires all agents running on other servers (including other NMAP Agents) to authenticate with the server before it carries out their requests. **NOTE:** NetMail agent authentication does not use clear-text passwords. By designating a messaging server as a trusted host, agents running on that server are not required to authenticate with the NMAP server. Rather, they are given open access to the NMAP Agent and its accompanying message queues and mail directories. Although not required, designating trusted hosts improves performance in distributed messaging systems. Changes to this property are effective within 5 minutes. **IMPORTANT:** Because trusted hosts have complete access to all mailboxes and queued messages, ensure that messaging servers with trusted host status are secure. Additionally, do not grand trusted host status to Linux machines unless login access to the trusted host machines is restricted to the system administrator.
Clients		This page lists all NetMail agents that are registered to the current NMAP Agent. Agents that are typically clients of the NMAP Agent are the POP, IMAP, Modular Web Agent, etc., regardless of whether they reside on the current messaging server or on a remote messaging server. This is an informational page; you cannot add agents to or delete agents from the list.
Status		By default, the NMAP Agent is enabled. To disable the NMAP Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the NMAP Agent at startup. However, to immediately disable the agent, you must manually unload NMAPD.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the NMAP Agent is disabled, the messaging server does not launch NMAPD.NLM again until you deselect The Disable agent option and restart the messaging server.
	Add	To add a trusted host, 1. Type the IP address of a messaging server hosting NetMail agents that need open access to the NMAP Agent. 2. Click Add. On NetWare, because 127.0.0.0 and localhost are automatically trusted hosts, you do not need to add them to the list.

Option		Function
	Minimum Message Size	The SCMS threshold for a message's minimum size, in kilobytes. If a message is larger than the designated message size and it exceeds the Minimum Number of Recipients threshold, it is stored in the SCMS directory.

Option		Function
	Trusted Clients of this NMAP Server	
	Remove	To remove a trusted host, select the trusted host > click Remove.

6 Configuring E-mail Services

To provide e-mail services to your users, you must have a mail client agent (POP, IMAP, or the Modular Web Agent) running on at least one messaging server in the network. Additionally, an SMTP Agent must run on at least one messaging server in the network to send and receive messages over the Internet.

Beyond these essential messaging components, you can provide your users with optional services such as message forwarding, autoreply messages, mail proxy, and system-wide address books.

This section helps you successfully create and configure your messaging system's e-mail services. Section topics include

- "POP Agent" on page 77
- "IMAP Agent" on page 79
- "Configuring a POP3 or IMAP4 E-mail Client" on page 81
- "Modular Web Agent" on page 81
- "Modular Web Agent Modules" on page 85
- "Templates" on page 89
- "SMTP Agent" on page 89
- "Calendar Agent" on page 99
- "AutoReply Agent" on page 101
- "Rule Agent" on page 102
- "Proxy Agent" on page 104
- "Address Book Agent" on page 106
- "AntiVirus Agent" on page 112

POP Agent

Description: Pop Agent icon

Use the POP3 protocol to retrieve messages. When the POP Agent retrieves a message, it usually downloads the message to the mail client on the user's computer and then deletes it from the user's mailbox on the messaging server. Consequently, POP3 mail clients must store all retrieved messages locally. While POP3 conserves space on the messaging server, mailbox items cannot be viewed anywhere but in the local client.

The following table illustrates how the POP Agent retrieves messages from the user's mailbox.

Stage	Agent	Description
1	 User	The mail client connects to the POP3 Agent and sends the username and password.
2	 directory	The POP Agent looks up the user in eDirectory™ and authenticates the user. The POP Agent also uses the MSG.API to determine the NMAP Agent to use to access the user's mailbox.
3	 NMAP Agent	The POP Agent creates a connection to the NMAP Agent that manages the user's mailbox.
4	 POP3 E-mail Client	Using the POP3 protocol, the e-mail client sends a request to the POP Agent to download messages.
5	 POP Agent	Using the NMAP protocol, the POP Agent sends the request to the appropriate NMAP Agent.
6	 NMAP Agent	The NMAP Agent accesses the user's NetMail mailbox, extracts the requested messages, and returns them to the POP Agent using the NMAP protocol.
7	 POP Agent	Using the POP3 protocol, the POP Agent then returns the messages to the POP3 e-mail client.
8	 POP3 E-mail Client	The POP3 e-mail client displays the messages from the user's NetMail mailbox.
9	 User	The user is able to read his or her messages in the POP3 e-mail client.

Creating a POP Agent

To create the POP Agent, select the messaging server on which you want to create the POP Agent and choose POP Agent from the Create menu.

After you create the POP Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the POP Agent

The only POP property is Status. To disable the POP Agent, mark Disable Agent > click OK in the agent Details menu.

Marking Disable Agent prevents the messaging server from launching the POP Agent program—POP3D.NLM at startup. However, to immediately disable the agent, you must manually unload POP3D.NLM or restart the messaging server. For information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

When the POP Agent is disabled, the messaging server does not launch POP3D.NLM again until you deselect the Disable Agent option and restart the messaging server.

POP Agent Contexts

Only those users that belong to the messaging system can download mail via the POP Agent. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services. If the username does not exist within the local messaging server's NMAP context list, the user is denied access to the messaging system.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

IMAP Agent

Description: IMAP Agent icon

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 mail client on the user's computer, but leaves a copy of the message in the user's mailbox on the messaging server. In fact, all user folders and messages are maintained on the messaging server. This means that users can access their folders and messages from any location. IMAP also allows concurrent access to a single mailbox by more than one IMAP client. The drawback is that, unless restricted, mailbox growth can quickly consume the messaging server's disk space.

The following table illustrates how the IMAP Agent retrieves messages from the user's mailbox.

Stage	Icon	Description
1	 User	The mail client connects to the IMAP Agent and sends the username and password.
2	 eDirectory	The IMAP Agent looks up the user in eDirectory and authenticates the user. The IMAP Agent also uses the MSG.API to determine the NMAP Agent to use to access the user's mailbox.

Stage	Icon	Description
3	 NMAP Agent	The IMAP Agent creates a connection to the NMAP Agent that manages the user's mailbox.
4	 IMAP Agent	Using the NMAP protocol, the IMAP Agent sends the request to the appropriate NMAP Agent.
5	 NMAP Agent	The NMAP Agent accesses the user's NetMail mailbox, extracts the requested messages, and returns them to the IMAP Agent using the NMAP protocol.
6	 IMAP Agent	Using the IMAP4 protocol, the IMAP Agent then returns the messages to the IMAP4 e-mail client.
7	 IMAP4 E-mail Client	The IMAP4 e-mail client displays the messages from the user's NetMail mailbox.
8	 User	The user is able to read his or her messages in the IMAP4 e-mail client and send messages in return.

Creating an IMAP Agent

To create the IMAP Agent, select the messaging server on which you want to create the IMAP Agent and choose IMAP Agent from the Create menu.

After you create the IMAP Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the IMAP Agent

The only IMAP property is Status. To disable the IMAP Agent, mark Disable Agent > click OK in the agent Details menu.

Marking Disable Agent prevents the messaging server from launching the IMAP Agent program—IMAPD.NLM at startup. However, to immediately disable the agent, you must manually unload IMAPD.NLM or restart the messaging server. For information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

When the IMAP Agent is disabled, the messaging server does not launch IMAPD.NLM again until you deselect the Disable Agent option and restart the messaging server.

IMAP Agent Contexts

Only those users that belong to the messaging system can download mail via the IMAP Agent. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services.If the username does not exist within the local messaging server's NMAP context list, the user is denied access to the messaging system.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

Configuring a POP3 or IMAP4 E-mail Client

Because Outlook* Express can be configured as either a POP3 or an IMAP4 e-mail client, we use it here as an example for configuring a POP3 or IMAP4 e-mail client.

For information on configuring other e-mail clients, such as Netscape* Communicator* or Eudora,* refer to the e-mail 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 e-mail via NetMail:

1. Start Outlook Express.
2. If you already have an existing Outlook Express account, click Tools > Accounts > Add, and then 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 e-mail address > click Next.
5. From the list box, select POP3 or IMAP, depending on the agents that are created on your NetMail messaging server.
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 NetMail system, the incoming mail server and outgoing mail server can be the same messaging server or different messaging servers.
8. Click Next.
9. Type your POP or IMAP account name and password > click Next.
10. Click Finish.

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

Modular Web Agent

Description: Modular Web Agent icon

The Modular Web Agent provides the browser-based interface to the NetMail mailbox and calendar. It allows users to send and receive mail; manage mail folders; search for e-mail addresses; maintain a calendar of appointments; create and accept appointments, notes, and tasks; and set their client preferences.

The following table illustrates how the Modular Web Agent interacts with the user's Web browser.

Stage	Icon	Description
1	 User	The user connects to his or her mailbox in the NetMail system from a Web browser.
2	 Web Browser	The Web browser requests the contents of the user's mailbox by communicating with the Modular Web Agent using HTTP.
3	 eDirectory	The Modular Web Agent receives the request, looks the user up in eDirectory, and authenticates the user. The IMAP Agent also uses the MSG.API to determine the NMAP Agent to use to access the user's mailbox.
4	 Modular Web Agent	Using the NMAP protocol, the Modular Web Agent sends the request to the appropriate NMAP Agent.
5	 NMAP Agent	The NMAP Agent accesses the user's NetMail mailbox and returns the contents to the Modular Web Agent using NMAP protocol.
6	 Modular Web Agent	Using HTTP, the Modular Web Agent then returns the mailbox contents to the Web browser.
7	 Web Browser	The Web browser displays the contents of the user's mailbox.
8	 User	The user is able to read and send messages in the Web browser.

Creating a Modular Web Agent

To create the Modular Web Agent, select the messaging server on which you want to create the Modular Web Agent and choose Modular Web Agent from the Create menu.

After you create the Modular Web Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the Modular Web Agent

From the Modular Web Agent's Details menu, you can configure the following options:

IMPORTANT: You must restart MODWEBD to effect any changes in the Modular Web Agent's configuration. See "Loading and Unloading NetMail Agents" on page 317 for more information.

Option		Function
Configuration		
Configuration		
	Identifier	The name of your company. This appears in the title bar of each client window.
	Default Language	The default language for the Modular Web Agent and its sub-modules. The language defined in the Parent object or User Preferences overrides this default setting.
	Default Timezone	The default time zone for the Modular Web Agent and its sub-modules. The time zone defined in the Parent object, User object, or User Preferences overrides this default setting.
Ports		
	HTTP Port	The port the Modular Web Agent uses for HTTP connections. The default HTTP port assignment is port 80 or, on Novell Nterprise Linux Services, port 52080. Use the default port number unless that port number is already in use by another program on the server. **IMPORTANT:** The NetWare® Management Portal also uses the default HTTP port assignment of 80. If you are running the NetWare Management Portal NLM on your messaging server (HTTPSTK.NLM), users are not able to reach the Modular Web Agent. For users to reach the Modular Web Agent, you must unload HTTPSTK.NLM from your Modular Web Agent server, change the NetWare Management Portal's port assignment, or change the Modular Web Agent's port assignment. Otherwise, when users type the Modular Web Agent server's IP address or hostname, they launch the NetWare Management Portal.
	HTTPS (SSL) Port	The port the Modular Web Agent uses for secure HTTP (HTTPS) connections. The default HTTPS port assignment is port 443 or, on Novell Nterprise Linux Services, port 52443. Use the default port number unless that port number is already in use by another program on the server.

Option		Function
Template		NetMail templates allow you to control the mail client interface. NetMail 3.5 ships with two client templates—WebAccess (Webacc.ctp) and Webmail (WebMail.ctp). The WebAccess interface provides standard mail client functionality, calendaring, assigning tasks, and writing notes. Administrators can also use the WebAccess interface to delegate NetMail administrative functions such as adding, modifying, and deleting user accounts. Webmail is the NIMS 2.5 mail client interface. It provides standard mail client functionality and administrators can use the Webmail interface to give users access to self-administration features like changing passwords and configuring vacation messages.
	Default Template	The template in use if no template is defined in the User and Parent objects. Select the default template from the Available Templates list.
	Available Templates	The list of available templates. To add templates to the list, 1. Click the Browse button (...). 2. Click Add to browse for additional templates. **NOTE:** To add a template to the list of available templates, you must first create the template object or an Alias of that object in the Template container.
Status		By default, the Modular Web Agent and its plug-in modules are enabled. To disable the Modular Web Agent and its plug-ins, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Modular Web Agent and its plug-in modules at startup. However, to immediately disable the agent and its plug-in modules, you must manually unload MODWEBD.NLM or restart the messaging server. For information on manually unloading NetMail agents or restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317. After the Modular Web Agent is disabled, the messaging server does not launch MODWEBD.NLM again until you deselect the Disable Agent option and restart the messaging server.

Modular Web Agent Contexts

Only those users that belong to the messaging system can access their NetMail mailbox through the Modular Web Agent. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services. If the username does not exist within the local messaging server’s NMAP context list, the user is denied access to the messaging system.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, “Configuring the NMAP Agent,” on page 68.

Accessing the Modular Web Client

The Modular Web Agent's templates, Webmail and WebAccess, are Web-based mail clients that allows users to send and receive messages from anywhere if they are connected to the Internet and have a Web browser.

To access the Modular Web Agent clients:

1. In your Web browser, type the URL or host name of the server where NetMail is installed.

   If the Modular Web Agent's port assignment has changed, you must follow the server's hostname or IP address with a colon and the new port assignment. For example:

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

2. To authenticate to the Modular Web Agent server, type your username and password.
3. Click OK.

   The client appears in the browser.

Modular Web Agent Modules

The Modular Web Agent is a container with object properties. Within the Modular Web Agent, you can create four modules:

- The Calendar Module enables the calendar features, including appointments, tasks, and notes. Calendar options are only available in the WebAccess interface.
- The Mail Module provides mail and address book functions.
- The Preferences Module allows users to change their password.
- The Task-Oriented Management Module enables task-oriented management functions such as adding, modifying, deleting, and importing user accounts through the WebAccess interface.

Creating the Modular Web Agent Modules

To create the Modular Web Agent modules, select the Modular Web Agent and choose the specific module from the Create menu.

After you create the module, you must restart the messaging server. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the Modular Web Agent Modules

The Modular Web Agent modules are configured through the Details menu in the same way as other Directory objects.

IMPORTANT: You must restart MODWEBD to effect any changes in the plug-ins' configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

An explanation of each module's configuration options is provided in the following sections.

Configuring the Calendar Module

The only Calendar Module property is Queue Server. From the Calendar Module's Details menu, you can configure Queue Server property:

Option	Function
Queue Server	The queue server is the NMAP Agent to which the ModWeb Calendar Module delivers appointments, notes, and tasks that the message queue needs to process. Each ModWeb Calendar Module can have only one queue server. Use the Browse button to select any NMAP Agent in the tree. If the ModWeb Calendar Module and NMAP Agent are not running on the same server, you can make the server running the ModWeb Calendar Module a trusted host of the NMAP Agent for faster server access. For more information, see the Trusted Hosts property in Table 4, “Configuring the NMAP Agent,” on page 68. To verify that the ModWeb Calendar Module is registered to a particular queue server, view the Client property in the NMAP object. If registered, the server running the ModWeb Calendar Module is listed as an NMAP client.

Configuring the Mail Module

From the Mail Module’s Details menu, you can configure the following options:

Table 3 Configuring the Mail Module

Option		Function
Options		
Limits		
	Maximum number of recipients per mail	Limits the number of recipients per message sent by users from the Modular Web Agent client. The ModWeb Mail Module does not restrict the number of recipients for inbound messages that the Modular Web Agent client downloads from the user’s mailbox.
	Message Size Limit	The maximum message size users can send from the Modular Web Agent. The ModWeb Mail Module does not restrict the size of inbound messages the Modular Web Agent downloads from the user’s mailbox.
Addressbook		The Addressbook options allow you to control which address books users can access from the Modular Web mail templates. **NOTE:** To sort the ModWeb address books, see “Configuring the Mail Module” on page 86.
	Personal	Allows Modular Web Agent users to create personal address books. Users’ personal address books are stored in their User object. Consequently, users can access their personal address book from any location as long as they are logged in to the network.

Option		Function
	System-Wide	If marked, this option gives users access to a system-wide address book in the Modular Web client (WebAccess or Webmail). In the LDAP URL field, you can type the following LDAP parameters: ldap://user:password@hostname:port/?basedn ◆ The *user:password* variable is the user's name and password. ◆ *Hostname* identifies the LDAP server's host name or IP address. If you type the IP address of a server running the Address Book Agent, users can access address book information from eDirectory. ◆ *Port* specifies the LDAP port assignment. If the LDAP server uses the default LDAP port (port 389), you do not need to specify a port. ◆ *Basedn* identifies the address book context. This is required if the Require DN attribute is added to the Address Book Agent. It is ignored if the Derive DN from Authentication is added to the Address Book Agent. (See "Address Book Agent Optional Features" on page 110 for more information.) Users with the Privacy attribute set to Limited or None in their User object are visible to other NetMail users in the System-Wide Addressbook. Users with an Unlisted privacy setting are not visible in the System-Wide Addressbook. **NOTE:** For information on providing domain-specific address books, see "Managing Multiple Address Books" on page 258.
	Public	If marked, this option allows users to define their own public address books in the Modular Web client (WebAccess or Webmail). To define a default Public LDAP Server, type the host name or IP address of any public LDAP server in the LDAP URL field. You can use the same LDAP parameters discussed under System-Wide LDAP Server.
Queue Server		The queue server is the NMAP Agent to which the ModWeb Mail Module delivers messages that the message queue needs to process. Each ModWeb Mail Module can only have one queue server. Use the Browse button to select any NMAP Agent in the tree. If the ModWeb Mail Module and NMAP Agent are not running on the same server, you can make the server running the ModWeb Mail Module a trusted host of the NMAP Agent to expedite server access. For more information, see the Trusted Hosts property in Table 4, "Configuring the NMAP Agent," on page 68. To verify that the ModWeb Mail Module is registered to a particular queue server, view the Client property in the NMAP object. If registered, the server running the ModWeb Mail Module is listed as an NMAP client.

Configuring the Mail Module to Sort Address Books

IMPORTANT: The following information only applies to ASCII-based languages.

Using a DS editing tool such as NDS Snoop, it is now possible to configure the Mail module to sort address books by first name or last name in the WebAccess and Webmail templates.

To sort the address book output by first name, add the following information to the MWMail configuration in eDirectory:

```
Attribute: Novonyx.Configuration
Value: SortAddressbook=1
```

To sort address book output by first and last name, use the following full MWMail configuration entry:

```
Attribute: Novonyx.Configuration
Value: SortAddressbook=1
Value: SortKey=L
```

NOTE: If you sort the address books by last name, consider redesigning your ModWeb template to display the last name before the first name.

Configuring the Preferences Module

From the Preference Module's Details menu, you can configure the following options:

Option		Function
Options		
Passwords		
	Allow Users to Change Password	Enables users to change their login password from the Modular Web Agent templates. Because NetMail is completely integrated with eDirectory, the user's ModWeb password is the same as the user's NetWare login password. Therefore, marking this option actually gives your users rights to their NetWare login password through Modular Web Agent, regardless of whether they have rights to the actual password property in their User object.
	SSL Required	Requires Modular Web Agent users to make an SSL connection to the server running the ModWeb Preferences Module before they can change their passwords. **NOTE:** You must have a server certificate installed on the current messaging server before you can enable this option. For information on setting up your server certificate, see "Setting Up TLS and SSL" on page 231.
Disable Options		Disables user configuration options in the WebAccess and Webmail templates. If marked, these options do NOT appear in the User Preferences menu.
	Timeout	The amount of idle time before the user is automatically logged out of the Modular Web client.
	Colors	Template color definition options. This option is specific to the Webmail template.
	Signature	Custom text automatically inserted at the end of each message.
	Privacy	The user's level of privacy within the messaging system. The privacy level controls what the Address Book Agent reveals about the user.

Configuring the Task-Oriented Management Module

This Task-Oriented Management Module has no configurable options. However, you must run it on the messaging server to enable TOM administration. See "Task-Oriented Management" on page 262 for more information on configuring TOM administration.

Templates

Description: Template icon

Templates control the appearance of the Modular Web Agent's mail client interface. By default, two templates ship with NetMail 3.5: WebAccess (Webacc.ctp) and Webmail (WebMail.ctp). The template files are found in the following directories:

Platform	Directory
NetWare	sys:\system\modweb
Windows	\program files\novell\netmail\bin\modweb
Linux	/opt/novell/netmail/bin/modweb/

Webacc.ctp and WebMail.ctp each contain everything needed to present their respective client interface; the HTML codes, program strings, language files, graphics, etc. are all compiled in this single file. Consequently, NetMail no longer needs to install multiple mail client directories. When the Modular Web Agent initializes on the messaging server, it simply loads the template files into memory.

You must create the WebAccess and Webmail objects in the tree before you can load them on the messaging server or select them in the Modular Web Agent, Parent, and User objects. Although the WebAccess and Webmail template objects can actually be created anywhere in the tree, creating them in the Template container makes it easier to locate and manage these objects.

Creating Template Objects

To create a Template object, select the Templates container (or the container in which you want to create the Template object) and choose Modular WebAgent Template from the Create menu. In creating the Template object, you are prompted to type the name of the template.

IMPORTANT: You must type either "WebAccess" or "Webmail" as the template name.

Template objects have no configurable options. After creating the WebAccess and Webmail Template objects, you can select them in the Modular Web Agent, Parent, and User objects.

SMTP Agent

Description: SMTP Agent icon

The SMTP Agent is the means by which messages enter and leave the NetMail messaging system via the Internet. Consequently, the SMTP Agent must run on at least one messaging server in the network in order to send and receive messages over the Internet.

NOTE: In addition to sending and receiving messages over the Internet, the SMTP Agent is required to send messages from POP and IMAP mail clients.

Creating an SMTP Agent

To create the SMTP Agent, select the messaging server on which you want to create the agent and choose SMTP Protocol from the Create menu.

In creating the SMTP Agent object, you are prompted for the following information:

Option	Function
Primary Domain	The Primary Domain is the Internet domain your organization uses. In the e-mail address “email_user@company.com,” for example, “company.com” is the Internet domain. By default, the SMTP Agent’s Primary Domain corresponds with the messaging server’s Official Domain Name.
Queue Server	The queue server is the messaging server that the SMTP Agent delivers messages in the queue for processing. A messaging server in the tree with an NMAP Agent is required. Use the Browse button to locate the queue server.

After you create the SMTP Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317.

Configuring the SMTP Agent

From the SMTP Agent’s Details menu, you can configure the following options:

Interface changes:
Under “Indentification,” “Other” replaces “Limits” as a new section header. Also “Parent Object” is not documented under this section

Under Options > Flags, the ui item names have changed slightly.

Under Options > Mail Relay Host, this has changed and need revised..

Under UBE Blocking > Flags, the ui item names have changed slightly..

Under UBE Blocking > RBL Check, the ui items have changed and need revised.

Under UBE Relaying > Flags, the ui items names have changed slightly.

Under UBE Relaying > Relaying, the ui items have changed and need revised. It appears that several items can be removed.

The table cells labelled “Domains” and “NetMail Parent Objects” are extras and don’t seem to fit with the new interface.

Table 4 Configuring the SMTP Agent

Option		Function
Identification		You must add all the domain and host names that your NetMail system is planning to accept messages in either the Global or Hosting Domains list. In listing the domains that belong to your messaging system, consider the following important points: ◆ Do not list a domain as both a Global Domain and a Hosting Domain. ◆ Failure to add all domain and host names that resolve to the server's IP address creates message loops that quickly consume all your server resources. The problem is that messages addressed to domains not included in the SMTP Agent's domain lists still resolve to the SMTP server's IP address. However, because they aren't listed in the domain lists, the SMTP Agent cannot accept them. Therefore, the SMTP server ends up relaying these messages to itself in an endless loop. (NetMail only prevents such loops for domains that resolve to loopback or the server's default IP address.)
	Domains	
	Global Domains	A listing of the messaging system's native domains. When the SMTP Agent receives a message, it looks at the domain portion of the recipient's e-mail address (everything after the @ symbol). If the addressed domain matches a domain in the Global Domains list, the SMTP Agent removes the domain portion of the address and drops the message in the message queue. Because the SMTP Agent removes Global Domains from the recipient's e-mail address, ensure that the user portion of the e-mail address (everything before the @ symbol) is unique. You can address unique usernames at any global domain. For example, messages addressed to Bob@Novell.com and Bob@Novell.edu are delivered to the same mailbox if Novell.com and Novell.edu are listed as Global Domains and a User object named "Bob" exists in an NMAP Agent context. (For more information on NMAP Agent contexts, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68. **IMPORTANT:** In NetMail 3.5, you do *not* need to restart the SMTP Agent after adding domains to the Global Domains list. New domains are recognized by the SMTP Agent within 5 minutes.

Option		Function
	Hosting Domains	A listing of foreign domains hosted on the current system. This option is most applicable to ISP environments. For more information, see "Hosting Domains" on page 250. When the SMTP Agent receives a message addressed to a domain in the Hosting Domains list, it drops the message in the message queue *without* removing the domain portion of the recipient's e-mail address. Because the entire e-mail address remains intact, it is not necessary that the user portion of the e-mail address (everything before the @ symbol) is unique. Combining the user's name with a Hosting Domain name enables identical users to exist within the same messaging system. Although, you might have multiple users named "jling" in your overall messaging system, each one has a unique NDS username. **NOTE:** Because the user's e-mail address is also the user's NDS username, the user must type his or her full e-mail address (*username*@*domain*) to log in to the system. **NOTE:** Users created with domains in their NDS object names can only be addressed at that domain. For example, messages addressed to Bob@Novell.com and Bob@Novell.edu are delivered to different mailboxes if Novell.com and Novell.edu are listed as Hosting Domains and NDS objects named Bob@Novell.com and Bob@Novell.edu exist in an NMAP Agent context. (For more information on NMAP contexts, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68..) In Hosting Domains, users can use Netscape Messenger 4.x in IMAP mode or they can manually configure the POP client to accept usernames with the @ symbol. To enable the Netscape Messenger* 4.*x* POP client to accept usernames with the @ symbol, edit the PREFS.JS file in the C:\PROGRAM FILES\NETSCAPE\USERS*USERNAME* directory. Add the following line above the other mail lines: user_pref("mail.allow_at_sign_in_user_name", true) You can then restart the Netscape Messenger 4.*x* POP client. It is possible to make this change before distributing the Netscape client to all the users. **IMPORTANT:** In NetMail 3.5, you do *not* need to restart the SMTP Agent after adding domains to the Hosting Domains list. New domains are recognized by the SMTP Agent within 5 minutes.
Limits		
	Message Size Limit	The maximum message size the SMTP Agent accepts. Because the SMTP Agent handles all Internet traffic, this property limits both incoming and outgoing Internet messages. You can type any amount between None (no limit) and 40 MB. Changes to this property are implemented within 5 minutes.
Options		
Flags		A series of standard SMTP commands that you can enable on the current SMTP Agent. Select the commands you want the SMTP Agent to accept. Changes to the STMP flags are implemented within 5 minutes.

Option		Function
	Allow Clients to Use VRFY Command	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 usernames. For example, if spammers want to find out the usernames in your company, they could query the system with a series of usernames until the system verified a valid username. When verifying that a user exists in the messaging system, the SMTP Agent references the context list maintained by the messaging server. If the user is not listed in the context list, the SMTP Agent returns a "User Not Found" message. See the Context property in Table 4, "Configuring the NMAP Agent," on page 68 for more information on the NMAP Agent's context list.
	Allow Clients to Use EXPN Command	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 makes a request to expand a system-wide group such as Everyone, the SMTP Agent returns the complete membership list, which is, essentially, every username in your organization.
	Verify Recipient Addresses When Accepting Messages	By default, the SMTP Agent accepts all incoming messages and places them in a queue where their addresses are verified, as resources are available. This process facilitates rapid message processing. However, if you want the SMTP Agent to perform address verification before accepting messages into your NetMail system, select Verify Addresses on Receipt. **IMPORTANT:** NetMail Aliasing does not work if Verify Recipient Addresses When Accepting Messages is selected. When this option is enabled, the SMTP Agent intercepts messages before they are processed in the message queue; consequently, messages addressed to NetMail aliases are deleted before the Alias Agent can process them. For more information on the Alias Agent, see "Managing User Aliases" on page 253.
	Send ETRN to Servers	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. For more information, see "Servicing ETRN Domains" on page 251.
	Accept ETRN from Clients	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. For more information, see "Servicing ETRN Domains" on page 251.
Mail Relay Host [Forwarder]		A mail relay host is a relay point for remote messages. Use it to transfer outbound messages through a firewall. ETRN Domains also use Mail Relay Hosts to transfer messages to their relay service. (See "Servicing ETRN Domains" on page 251 for more information.) **IMPORTANT:** You must restart SMTPD to effect any changes in the Mail Relay Host configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option		Function
	Use Relay Host	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 you plan to use as the mail relay host. All remote messages going through this SMTP Agent are then forwarded to the SMTP Agent at the designated address.
UBE Blocking		This page provides options that block incoming messages from specified sites. These options are designed to protect your messaging system from unsolicited bulk e-mail (UBE) or SPAM. Changes to these properties are implemented within 5 minutes.
Flags		
	Do Not Allow Access from Hosts in Blocked List	Restricts access to your messaging system. If selected, the SMTP Agent refuses connections from any mail host with an IP address designated in the Blocked Hosts list.
	Deny Access to Hosts Not in DNS	Provides reverse DNS lookups. When receiving messages from external systems, the SMTP Agent verifies that the host's IP address and domain correspond to its DNS record. If they don't match, the SMTP Agent drops the connection. **NOTE:** You must configure your DNS server to support reverse DNS lookups for this option to function.
	Override with Authentication	This option provides an exception to the Deny Access to Hosts Not in DNS option. If marked, hosts that are not listed in DNS are given the opportunity to authenticate with the SMTP Agent before their connection is dropped.
RBL Check		Enables the SMTP Agent to do lookups on the Realtime Blackhole List (RBL*). RBL maintains a list of confirmed spammers and open relays. If the mail host matches an entry on the RBL, the connection is refused. To enable this option, mark Perform Check.

Option		Function
	Add	To add an RBL site, type the IP address or host name of the RBL list server and click Add. The RBL entry can include a trailing semi-colon (;) and subsequent text. The text following the semi-colon is displayed as part of the protocol reply informing the sender he is blocked. The following configuration entry references bl.spamcop.net as the RBL Host and then adds a message directing the sender to the SpamCop web site. bl.spamcop.net;You have been blackholed by spamcop.net. Please see http://spamcop.net to get removed If the character sequence *%d.%d.%d.%d* is entered as part of the text, it is replaced by the IP address of the blocked system. Use this feature to generate responses containing URLs that point directly to the RBL system's look-up page. For example, in this configuration entry, bl.spamcop.net;Please see http://spamcop.net/w3m?action=checkblock&ip=%d.%d.%d.%d http://spamcop.net/w3m?action=checkblock&ip is the URL format for SpamCop's lookup page and *%d.%d.%d.%d* generates the IP address of the blocked host. The resulting protocol reply includes a URL that takes the blocked sender directly to SpamCop's lookup page and tests his or her IP address. **IMPORTANT:** If a percent sign (%) is entered as part of the SMTP message text, type it as %%. Using a single percent sign without the letter "d" can crash the SMTP Agent.
	Delete	To remove an RBL site, select the site in the RBL list and click Delete.
	Blocked Hosts	A list of blocked IP address ranges. If Do Not Allow Access from Hosts in Blocked List is selected, the SMTP Agent refuses connections from any host within the designated IP address range. Listing ranges of registered IP addresses blocks specific external hosts from sending mail to or relaying mail through your messaging system. For example, you can choose to list the IP addresses registered to public mail systems (such as Hotmail,* Yahoo,* and Juno*) because spammers frequently use these systems to relay UBE. Use this option to block internal hosts. By listing ranges of internal IP addresses, you can block specific workstations from sending any messages over the Internet.
	Add	To add a range of IP addresses to the Blocked Hosts list, 1. Type a range of disallowed IP addresses. For example: 251.70.2.53-251.70.2.60 2. Click Add. Repeat for each additional range of disallowed IP addresses. If you are using WebAdmin, provide only one range per line.

Option		Function
	Delete	To delete a range of IP addresses from the Blocked Hosts list, 1. Select the range. 2. Click Delete.
UBE Relaying		This page provides options that prevent spammers from using your messaging system to relay unsolicited bulk e-mail (UBE) or SPAM. Changes to these properties are implemented within 5 minutes.
Flags		
	SMTP-after-POP	Prohibits users from sending remote messages through the SMTP Agent until they have first authenticated with the messaging system via their POP3 or IMAP4 client. This works for most Internet e-mail clients because these clients always check for e-mail (log in) just before sending messages. This feature also includes the username of the person who authenticated with the messaging system in the message header. This helps track spammers who authenticate with a valid username but fake the message header to mask their identity. SMTP-after-POP requires that you run the Connection Manager Agent and that you configure the Conn. Mgr. option on the messaging server running the SMTP Agent. See “SMTP-after-POP” on page 232 for detailed instructions on configuring SMTP-after-POP authentication.
	Only Allow Remote Sending for Authenticated Senders	Enables Extended SMTP (ESMTP) authentication. If selected, the e-mail client must authenticate through the ESMTP protocol before the SMTP Agent relays its messages to remote recipients. Netscape Communicator* and Outlook* Express support ESMTP authentication. If both SMTP-after-POP and ESMTP authentication are enabled, they function as an either/or option. If a mail client does not authenticate via POP or IMAP when downloading mail, it must authenticate via ESMTP before it can send remote messages.
	Require Sender to Be in Allowed List for Remote Sending	Restricts access to your NetMail system by selectively allowing access. If marked, only mail hosts with an IP address designated in the Allowed Hosts list can relay remote messages through the current SMTP server. If SMTP-after-POP, ESMTP authentication, and Require Sender to Be in Allowed List for Remote Sending are all enabled, they function as an either/or option. If an e-mail client does not authenticate using of POP or IMAP when downloading mail, it must authenticate using ESMTP or the Allowed Hosts list must include it before it can send remote messages.
	Maximum Number of Recipients per mail	Restricts the number of users who can receive the same message. This option affects both inbound and outbound Internet messages. If a message exceeds the threshold, the SMTP Agent begins at the top of the recipient list and sends the message to the number of recipients designated in this field. You can also configure the ModWeb Mail Module to restrict the number of recipients per message sent by users in the Modular Web client. For information on the ModWeb Mail Module, see “Configuring the Mail Module” on page 86.

Option		Function
Relaying		
	Allowed Hosts	A list of allowed IP address ranges. If Require Sender to Be in Allowed List for Remote Sending is selected, only hosts that fall within the designated IP address ranges are allowed to send messages to remote recipients via the current SMTP Agent. 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. In addition to preventing external hosts from relaying messages through your messaging system, you can use the Allowed Hosts lis to prevent internal hosts from relaying remote messages. To restrict which workstations outside your organization that you allow to send remote messages, designate ranges of internal IP addresses. **NOTE:** If a workstation's IP address is not in an Allowed Hosts range, you can still use the workstation to send messages to users within the local messaging system.
	Add	To add a range of IP addresses to the Allowed Hosts list, 1. Type a range of allowed IP addresses. For example: 251.70.2.53-251.70.2.60 2. Click Add. Repeat for each additional range of allowed IP addresses. If you are using WebAdmin, provide only one range per line.
	Delete	To delete a range of IP addresses from the list, 1. Select the range. 2. Click Delete.
	Relayed Domains (ETRN)	ETRN Domains are messaging systems that use a hosting service, such as an ISP or ASP, to send and receive messages over the Internet. These systems have their own messaging servers, agents, and mail directories; however, all their messaging services are local. Consequently, they must use a hosting service to send and receive remote messages. In most instances, ETRN Domains have non-persistent dial-up connections to their ISP or ASP. For more information on ETRN Domains, see "Servicing ETRN Domains" on page 251.
	Domain(s)	The current SMTP Agent services the ETRN Domains. To support these domains, you must click the Accept ETRN option in the Options page.

Option		Function
Queue Server		The queue server is the NMAP Agent to which the SMTP Agent delivers messages that the message queue needs to process. Each SMTP Agent can only have one queue server. Use the Browse button to select any NMAP Agent in the tree. If the SMTP and NMAP Agents are not running on the same server, you can designate the SMTP server as a trusted host of the NMAP Agent server for faster access. For more information, see the Trusted Hosts property in Table 4, “Configuring the NMAP Agent,” on page 68. To verify that a List Agent is registered to a particular queue server, view the Client property in the NMAP object. If registered, the server running the SMTP Agent is listed as an NMAP client. **IMPORTANT:** You must restart SMTPD to effect any changes in the Queue Server configuration. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)
Monitored Queues		A monitored queue is the message queue from which the SMTP Agent picks up messages for remote delivery. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single SMTP Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. **NOTE:** You cannot configure multiple SMTP Agents to monitor the same queue. Only one SMTP Agent can monitor each queue. To verify that an SMTP Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the SMTP Agent is listed as an NMAP client. Changes to this property are implemented within 5 minutes.
	NetMail Parent Object	The Parent object associated with the SMTP Agent. The SMTP Agent recognizes all Global and Hosting Domains listed in its associated Parent objects. See “Supporting Multiple Internet Domains” on page 247 for more information. Changes to this property are implemented within 5 minutes.
Status		By default, the SMTP Agent is enabled. To disable the SMTP Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the SMTP Agent at startup. However, to immediately disable the agent , you must manually unload SMTPD.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317. After the SMTP Agent is disabled, the messaging server does not launch SMTPD.NLM again until you deselect the Disable Agent option and restart the messaging server.

SMTP Agent Contexts

By default, the SMTP Agent does not reference the NMAP Agent's context list when sending or receiving remote messages.

The only two instances in which the SMTP Agent references the context list are if VRFY or Only allow remote sending for authenticated senders are marked. For a more detail explanation, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

If the VRFY option is marked, the SMTP agent references the local context list to verify that a user exists in the local messaging system. If the user is not listed in the Agent's local context list, it returns a "User Not Found" message.

If Only allow remote sending for authenticated senders is marked, only those users that belong to the messaging system can send remote mail via the SMTP Agent. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services.

Calendar Agent

Description: Calendar Agent icon

The Calendar Agent provides automatic status tracking information for scheduled appointments, tasks, and notes. When a user schedules a calendar event, the Calendar Agent processes all "Accept" and "Decline" responses and automatically updates the event's status information in the event organizer's calendar.

NOTE: Only the user who schedules the event can view who has accepted or declined a calendar event. Attendees only see their own status; every other attendee is viewed as pending. This design avoids the spikes in network traffic that would occur if every attendee updated every other attendee's status.

If you choose not to run the Calendar Agent, users receive iCal status messages in their Inbox. Because the status information is in iCal format, the event organizer might not be able to discern whether a recipient has accepted or declined the appointment.

NOTE: iCal mail clients, such as Microsoft Outlook XP, also provide automatic status tracking for scheduled appointments. If you are exclusively using an iCal compliant mail client, you can choose to either have NetMail manage status tracking via the Calendar Agent or to have the mail client manage status tracking.

If you are using the Modular Web client, you must run the Calendar Agent to provide automatic status tracking for scheduled appointments.

NOTE: Currently, NetMail does not support real-time scheduling with other systems; instead, calendaring information is exchanged via SMTP. This is due to the current lack of a ratified real-time calendar protocol. As soon as the proposed standard protocol (CAP) is ratified, NetMail plans to support real-time scheduling and busy searches.

Creating a Calendar Agent

To create the Calendar Agent, select the messaging server on which you want to create the agent and choose Calendar Agent from the Create menu.

In creating the Calendar Agent, you are prompted for the following information:

Option	Function
Store to be monitored	The Store to be monitored is the message queue serviced by the Calendar Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single Calendar Agent can monitor multiple message queues. However, you can only select one monitored queue when creating the Calendar agent. You can add multiple monitored queues when configuring the agent.

After you create the Calendar Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the Calendar Agent

From the Calendar Agent's Details menu, you can configure the following options:

Option	Function
Monitored Queues	A monitored queue is the message queue serviced by the Calendar Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single Calendar Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. **NOTE:** You cannot configure multiple Calendar Agents to monitor the same queue. Only one Calendar Agent can monitor each queue. To verify that an Calendar Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the Calendar Agent is listed as an NMAP client. **IMPORTANT:** You must restart CALAGENT to effect any changes in the Monitored Queues configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Status	By default, the Calendar Agent is enabled. To disable the Calendar Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Calendar Agent at startup. However, to immediately disable the agent , you must manually unload CALAGENT.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Calendar Agent is disabled, the messaging server does not launch CALAGENT.NLM again until you deselect the Disable Agent option and restart the messaging server.

Calendar Agent Contexts

The Calendar Agent only provides appointment status tracking information for users that belong to the messaging system. For standalone messaging servers, this means the user must belong to a

local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services. If the username does not exist within the local messaging server's NMAP context list, the user cannot determine who has accepted or declined the appointment by viewing the appointment in his or her calendar.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

AutoReply Agent

Description: AutoReply Agent

The AutoReply Agent lets users create custom messages that are automatically sent in response to incoming mail. For example, when users go on vacation, they can create a message that lets others know they are unavailable.

The AutoReply Agent also enables users to forward their messages to another e-mail address. Users can specify if they want to retain a copy of the message in their NetMail mailbox or forward the message to the designated address.

In addition to forwarding messages to another e-mail address, the AutoReply Agent can forward SMS messages to cellular phones and pagers. While it does not configure SMS messages, the AutoReply Agent can recognize a message's format and forward it to the user's designated cellular phone or pager number.

The AutoReply Agent is not client-specific. Although users must configure mail forwarding and autoreply messages in WebAccess, the agent functions independently of any e-mail client because users' forward and autoreply information is stored in their NDS User objects. Therefore, NetMail can handle forwarding and autoreply messages for users of POP3, IMAP4, and WebAccess clients.

Creating an AutoReply Agent

To create the AutoReply Agent, select the messaging server on which you want to create the agent and choose AutoReply Agent from the Create menu. In creating the AutoReply Agent, you are prompted for the following information:

Option	Function
Store to be monitored	The Store to be monitored is the message queue serviced by the AutoReply Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AutoReply Agent can monitor multiple message queues. However, you can only select one monitored queue when creating the Autoreply Agent. You can add multiple monitored queues when configuring the agent.

After you create the AutoReply Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the AutoReply Agent

From the AutoReply Agent's Details menu, you can configure the following options:

Option	Function
Monitored Queues	A monitored queue is the message queue serviced by the AutoReply Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AutoReply Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. **NOTE:** You cannot configure multiple AutoReply Agents to monitor the same queue. Only one AutoReply Agent can monitor each queue. To verify that an AutoReply Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the AutoReply Agent is listed as an NMAP client. **IMPORTANT:** You must restart FORWARD to effect any changes in the Monitored Queues configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Status	By default, the AutoReply Agent is enabled. To disable the AutoReply Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the AutoReply Agent at startup. However, to immediately disable the agent , you must manually unload FORWARD.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the AutoReply Agent is disabled, the messaging server does not launch FORWARD.NLM again until you deselect the Disable Agent option and restart the messaging server.

AutoReply Agent Contexts

Only those users that belong to the messaging system can forward mail or send autoreply messages via the AutoReply Agent. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services. If the username does not exist within the local messaging server's NMAP context list, the user cannot forward mail or send autoreply messages.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

Rule Agent

Description: Rule Agent icon

The Rule Agent executes rules defined in the WebAccess client.

The Rule Agent is not e-mail client specific. Although users must configure rules in WebAccess, the agent functions independently of any e-mail client because users' rules are stored in their NDS User objects. Therefore, NetMail executes the configured rules whether the users open their messages in a POP3, IMAP4, or WebAccess client.

Creating a Rule Agent

To create the Rule Agent, select the messaging server on which you want to create the agent and choose Rule Agent from the Create menu.

In creating the Rule Agent object, you are prompted for the following information:

Option	Function
Store to be monitored	The Store to be monitored is the message queue serviced by the Rule Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single Rule Agent can monitor multiple message queues. However, you can only select one monitored queue when creating the Rule agent. You can add multiple monitored queues when configuring the agent.

After you create the Rule Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the Rule Agent

From the Rule Agent's Details menu, you can configure the following options:

Option	Function
Monitored Queues	A monitored queue is the message queue serviced by the Rule Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single Rule Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. **NOTE:** You cannot configure multiple Rule Agents to monitor the same queue. Only one Rule Agent can monitor each queue. To verify that a Rule Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the Rule Agent is listed as an NMAP client. **IMPORTANT:** You must restart RULESRV to effect any changes in the Monitored Queues configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option	Function
Status	By default, the Rule Agent is enabled. To disable the Rule Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Rule Agent at startup. However, to immediately disable the agent , you must manually unload RULES.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Rule Agent is disabled, the messaging server does not launch RULES.NLM again until you deselect the Disable Agent option and restart the messaging server.

Rule Agent Contexts

Only those users that belong to the messaging system can configure message rules via the Rules Agent. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services. If the username does not exist within the local messaging server's NMAP context list, the user cannot configure message rules.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

Proxy Agent

Description: Proxy Agent icon

The Proxy Agent allows users to manage several e-mail accounts from a central mailbox. Users can retrieve messages from up to three POP3 or IMAP4 e-mail accounts on other messaging systems. (The Proxy Agent cannot retrieve messages from mail systems that do not provide POP3 or IMAP4 access to their mailboxes.) All messages retrieved from these accounts are stored in the user's NetMail mailbox as if it were the original destination.

Depending on the user settings, you can leave a copy of retrieved messages in the original mailbox or delete the messages from the host server. All proxy information is stored in the user's NDS User object.

Creating a Proxy Agent

To create the Proxy Agent, select the messaging server on which you want to create the agent and choose

Proxy Agent

from the Create menu.

In creating the Proxy Agent object, you are prompted for the following information:

Option	Function
Store to reference	The Store to reference option identifies which NDS contexts are serviced by the Proxy Agent. Users belonging to contexts supported by the selected NMAP Agent can proxy other mail accounts. Use the Browse button to locate and select an NMAP Agent. **NOTE:** At this point, you can only select one NMAP Agent; however, when configuring the Proxy Agent, you can add multiple NMAP Agents.

After you create the Proxy Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the Proxy Agent

From the Proxy Agent's Details menu, you can configure the following options:

Under Configuration, the un item names have changed slightly.
The "Monitored Servers" tab is now renamed "Monitored Queues"

IMPORTANT: You must restart MAILPROX to effect any changes in the Proxy Agent's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option		Function
Configuration		
	Run pickup every ___ hours	The number of hours that elapse between each message retrieval cycle.
	Pickup Threads	The number of threads you want to use to simultaneously retrieve messages. The more threads, the faster the message retrieval, but additional threads consume additional server memory.
Queue Server		The queue server is the NMAP Agent to which the Proxy Agent delivers messages that the message queue needs to process. Each Proxy Agent can only have one queue server. Use the Browse button to select any NMAP Agent in the tree. If the Proxy and NMAP Agents are not running on the same server, you can make the server running the Proxy Agent a trusted host of the NMAP Agent to expedite server access. For more information, see the Trusted Hosts property in Table 4, "Configuring the NMAP Agent," on page 68. To verify that a Proxy Agent is registered to a particular queue server, view the Client property in the NMAP object. If registered, the server running the Proxy Agent is listed as an NMAP client.
Monitored Servers		Monitored Servers are the messaging system contexts serviced by the Proxy Agent. Because NMAP Agents determine the messaging system's contexts, Monitored Servers correspond to NMAP Agents. Users belonging to contexts supported by the selected NMAP Agents can proxy other mail accounts. Use the Browse button to locate and select one or more NMAP Agents.

Option	Function
Status	By default, the Proxy Agent is enabled. To disable the Proxy Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Proxy Agent at startup. However, to immediately disable the agent , you must manually unload MAILPROX.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Proxy Agent is disabled, the messaging server does not launch MAILPROX.NLM again until you deselect the Disable Agent option restart the messaging server.

Proxy Agent Contexts

Only those users that belong to the messaging system can retrieve messages from POP3 or IMAP4 e-mail accounts on other messaging systems via the Proxy Agent. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services. If the username does not exist within the local messaging server's NMAP context list, the user cannot proxy messages.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

Address Book Agent

Description: Address Book Agent icon

The Address Book Agent provides read-only LDAP3 access to NDS. Using this agent, any LDAP-compliant application (such as e-mail or address book clients) can access address book information from NDS. Information returned about each user depends on the user's level of privacy as defined in WebAccess.

To speed up LDAP queries, the Address Book Agent maintains an index of all users in its supported NDS contexts. This index contains the user's e-mail address, first name, last name, and full name. Although the index contains the user's address book information, the Address Book Agent only uses the index to locate users in the tree. By default, all address book information, including the user's e-mail address, is taken from the User object in NDS. This means the address book is always as current as NDS.

This mode of inquiry is so fast that it is possible to use the Address Book Agent with the address type-ahead feature in many popular e-mail clients. Moreover, 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 also generate address book files. Use these LDIF files to distribute address book information to messaging systems (such as remote sites) that do not have access to the Address Book Agent.

NOTE: Do not confuse the Address Book Agent with the Modular Web Agent's address book feature. The Modular Web Agent address book is a user feature that can look up information in virtually any LDAP-compliant database. The Address Book Agent enables address book clients (such as the Modular Web Agent address book) to query NDS for address book information.

Using the Novell LDAP Server instead of the Address Book Agent

If you want to provide more address book information than that returned by the Address Book Agent (i.e., e-mail address, first name, last name, and full name), you can use the Novell® LDAP server instead of the Address Book Agent. While the LDAP server is NetWare-specific, it can return all the user information stored in the NDS User object.

If you use the LDAP server, ensure that the Internet E-mail Address field in the User object is populated or the LDAP server cannot return the Internet E-mail Address attribute (user's e-mail address).

The Address Book Agent also reads the Internet E-mail Address attribute stored in the User object; however, if this attribute is empty, it dynamically generates the user's e-mail address as follows:

- If the user belongs to a Hosting Domain, the Address Book Agent simply uses the username as the e-mail address.
- If the user belongs to a Global Domain, the Address Book Agent generates the e-mail address from the username and the user's Internet domain (username@domain).

To identify the user's Internet domain, the Address Book Agent looks in the following objects:

If the user is associated with a Parent object, the Address Book Agent looks in the Parent object's Global Domains list.

If no Global Domain is configured in the Parent object, the agent looks for the user's Container Domain.

If no Container Domain is configured, the Address Book Agent uses the messaging server's Official Domain.

IMPORTANT: ModWeb does not verify that the domain listed in the User object's Internet E-mail Address property is a supported Global or Hosting domain. Therefore, it is recommended you use the Alias Agent to populate this property or manually ensure the domain is valid.

Creating the Address Book Agent

To create the Address Book Agent, select the messaging server on which you want to create the agent and choose Address Book Agent from the Create menu.

In creating the Address Book object, you are prompted for the following information:

Option	Function
NMAP Context to be serviced	The NMAP Agent which the Address Book Agent references to generate its user index. Users belonging to contexts supported by the selected NMAP Agent are included in the agent's address book. Conversely, User objects not included in a supported context are not included in the agent's index and, therefore, are not available for address book queries. You can use the Browse button to locate and select an NMAP Agent.

After creating the Address Book Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317.

Configuring the Address Book Agent

From the Address Book Agent’s Details menu, you can configure the following options:

Under Configuration, the items have changed and the doc needs revised.

“The Monitored Queues” tab replaces “Monitored Servers.”

IMPORTANT: You must restart MSGLDAP to effect any changes in the Address Book Agent’s configuration. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)

Option	Function
Configuration	
Scheduler	

Option		Function
	Automatically Create Database Every _____ Day(s)	How often (in days) the Address Book Agent recreates the address book index. The default is one day. The maximum setting is 99 days. To speed up LDAP queries, the Address Book Agent maintains an index of all the information queried for any user in its supported NMAP contexts—specifically, the users' e-mail addresses, first names, last names, and full names. Although the index contains the user's address book information, the Address Book Agent only uses the index to locate users in the tree. By default, all address book information, including the user's e-mail address, is taken from the User object in NDS. This means the address book is always as current as NDS. **IMPORTANT:** ModWeb does not verify that the domain listed in the User Object's Internet E-mail Address property is a supported Global or Hosting domain. Therefore, it is recommended you use the Alias Agent to populate this property or manually ensure the domain is valid. If the user's e-mail address is not defined in the User object's Internet E-mail Address property, the Address Book Agent dynamically generates the e-mail address as follows: ◆ If the user belongs to a Hosting Domain, the Address Book Agent simply uses the username as the e-mail address. ◆ If the user belongs to a Global Domain, the Address Book Agent generates the e-mail address from the username and the user's Internet domain (username@domain). To identify the user's Internet domain, the Address Book Agent looks in the following objects: 1. If the user is associated with a Parent object, the Address Book Agent looks in the Parent object's Global Domains list. 2. If no Global Domain is configured in the Parent object, the agent looks for the user's Container Domain. 3. If no Container Domain is configured, the Address Book Agent uses the messaging server's Official Domain.
	LDAP/LDIF	
	Enable LDAP Lookup Server on Port	Specifies the Address Book Agent's LDAP port assignment. LDAP applications (such as the Modular Web Client Address Book) access the Address Book Agent via this port for address book lookups. The Address Book Agent's default LDAP port assignment is 389 or, on Novell Nterprise Linux Services, port 52389.

Option		Function
	Enable Automatic LDIF File Export	Configures the Address Book Agent to automatically create an LDIF (LDAP Data Interchange Format) file of all user information, except information or accounts protected by User object privacy settings. Use this file to distribute address book information to messaging systems (such as remote sites) that do not have access to the Address Book Agent. The LDIF file is created as ADDRBOOK.LDF in the following directories: ◆ sys:\PUBLIC on NetWare systems ◆ \DBF\Shared on Windows systems The LDIF file is automatically regenerated every time the Address Book Agent updates its user index.
	Allow Personal addressbook search	LDAP searches the user's personal address book if the LDAP connection is authenticated. For example, to authenticate the LDAP connection in Outlook Express*, the user must configure "My LDAP Server requires authentication" and type his or her NDS username and password.
Monitored Servers		Monitored servers are the NMAP Agents the Address Book Agent references to generate its index. Only those users belonging to contexts supported by the selected NMAP Agents are queried via the Address Book Agent. Conversely, User objects not included in a supported context are not included in the agent's index and, therefore, are not available for address book queries. Use the Browse button to locate and select one or more NMAP Agents.
Status		By default, the Address Book Agent is enabled. To disable the Address Book Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Address Book Agent at startup. However, to immediately disable the agent , you must manually unload MSGLDAP.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Address Book Agent is disabled, the messaging server does not launch MSGLDAP.NLM again until you deselect the Disable Agent option and restart the messaging server.

Address Book Agent Optional Features

Using a DS editing tool such as NDS Snoop, you can enable additional features in the Address Book Agent by modifying the value of the Novonyx:LDAP Options attribute.

The following table outlines all the options associated with the Novonyx:LDAP Options attribute.

Table 3 NovonyxLDAP Options, Value, and Description

Option	Value	Description
LDAP_SERVER_ON	1	This option is associated with the Status feature in the administrative interface.
LDIF_EXPORT_ON	2	This option is associated with the Enable Automatic LDIF File Export feature in the administrative interface.
LDAP_REQUIRE_BASEDN	4	This is the optional feature, Require Search Domain. It requires that a Search Domain is included in the address book configuration. Specify the Search Domain in the LDAP server's URL or in the address book client. See Options (Default LDAP server) in Table 3, "Configuring the Mail Module," on page 86 for information on specifying the Search Domain in the LDAP URL.
LDAP_REQUIRE_AUTHENTICATION	8	This is the optional feature, Require Authentication. It requires a username and password when users connect to the Address Book Agent.
LDAP_USE_USERS_BASEDN	16	This is the optional feature, Derive Search Domain from Authentication. It configures the Address Book Agent to derive the user's Search Domain from the username given during authentication. The Search Domain is essentially an address book filter. If this option is marked, the user can only view users from his or her domain. For example, if sally@abc.com authenticates with the Address Book Agent, she is only able to view users from abc.com in her address book. If you leave the Context field blank, the Address Book Agent manifests every user in the messaging system. The Address Book Agent can easily identify the Search Domain for users belonging to Hosting Domains because the domain is included in the username given during authentication. However, if the user belongs to a Global Domain, identifying the Search Domain is a little more complicated. The Address Book Agent looks in the following objects to identify a user's Global Domain: 1. If the user is associated with a Parent object, the Address Book Agent looks in the Parent object's Global Domains list. 2. If no Global Domain is configured in the Parent object, the agent looks for the user's Container Domain. 3. If no Container Domain is configured, the Address Book Agent uses the messaging server's Official Domain.
LDAP_SEARCH_PERSONAL	32	This option is associated with the Allow Personal addressbook search feature in the administrative interface.

The value of the Novonyx:LDAP Options attribute is calculated by adding the values of the enabled features. For example, to enable the LDAP server, require user authentication, and allow users to search their personal address book, you would store 41 (1+8+32) in the Novonyx:LDAP Options attribute.

Address Book Agent Contexts

Only those users that belong to the messaging system are listed in the Address Book Agent's system address book. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services.If the username does not exist within the local messaging server's NMAP context list, no address book information is available on that user.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.

AntiVirus Agent

Description: AntiVirus Agent icon

The NetMail AntiVirus Agent integrates with McAfee* NetShield*, Command* Antivirus, Computer Associates* InnoculateIT*, and Symantec* CarrierScan* virus engines to provide virus scanning on messages handled by NetMail.

If a message contains a virus, the AntiVirus Agent immediately deletes it from the message queue. You can configure the agent to return the message to the sender with a notice indicating which virus the message contained. It can also send a virus alert to the message recipient(s), indicating who tried to send the message and which virus the message contained.

You can enable virus scanning for all users in the messaging system or it can be limited to a group of users for whom virus scanning is enabled. Limiting virus scanning to specific users is most applicable to ISP environments where users can subscribe to this service.

NOTE: Virus scanning is enabled at the Parent or User objects.

For information on creating and configuring the AntiVirus Agent, see "Providing AntiVirus Protection" on page 240.

7 Using WebAccess and Webmail

With Novell® NetMail, you can use your existing POP or IMAP mail client or use the browser-based client interfaces included with NetMail. NetMail provides two client interfaces:

- WebAccess provides a full-featured interface that takes advantage of 4.x and higher browsers.
- Webmail is a more basic interface that requires no JavaScript support and runs within any browser that is compatible with HTML 2.0+ and above.

A test implementation of NetMail that demonstrates the client interfaces and offers free mail accounts is available at the MyRealBox Web site (http://www.myrealbox.com).

This section provides basic information on using WebAccess and Webmail.

- "Getting Started" on page 113
- "Using WebAccess" on page 114
- "Using Webmail" on page 155

NOTE: This section is written from a user perspective. As an administrator, you can extract this information and distribute it to your users.

Getting Started

WebAccess and Webmail are easy-to-use, Web-based e-mail interfaces that provide a wide range of powerful communication and collaboration capabilities including scheduling resources, busy search, shared folders, and proxy.

By default, WebAccess and Webmail give each user a default Inbox, calendar, and, if enabled, personal, shared and public address books. Users can then customize their mail account by creating multiple mail folders and calendars.

WebAccess and Webmail also provide the following mail items:

- **Mail Messages** are the standard e-mail messages and allow you to send attachments.
- **Appointments** allow you to schedule the time, date, and place of the appointment. Appointments are calendar items, which means accepted or personal appointments appear in the calendar. Also, recipients can choose to accept, decline, or delegate received appointments.
- **Tasks** allow you to indicate the day you want the task to appear in the recipient's calendar and the day you want the task completed. Tasks are calendar items, which means accepted or personal tasks appear in the calendar. Also, recipients can choose to accept, decline, or delegate received task. After the task is completed, recipients can mark the task completed.
- **Notes** allow you to indicate the day you want the note to appear on the recipient's calendar. Notes are calendar items, which means accepted or personal notes appear in the calendar. Because notes are posted in the recipient's calendar, you can use them as reminders of specific

events, such as days off, project deadlines, or birthdays. Also, recipients can choose to accept, decline, or delegate received notes.

You address mail messages using the Address Book to add recipients' addresses to the To, CC, and BC boxes. You address appointments, tasks, and notes using the Address Book to add recipients' addresses to the Required, Optional, or Not Attending boxes. You can also include Web site locations (URLs) in the Subject and Message box of each item

Using WebAccess

WebAccess is for use with higher-end browsers that support Java* scripting.

NOTE: If your browser is a lower-end browser, use the Webmail interface instead. To change to the Webmail interface, see "Changing from WebAccess to Webmail" on page 153.

This section covers the following tasks:

- "Starting and Exiting the WebAccess Interface" on page 114
- "Viewing and Sending Mail Messages" on page 115
- "Forwarding Items" on page 118
- "Replying to Items" on page 119
- "Scheduling Appointments and Using the Calendar" on page 121
- "Using Tasks" on page 128
- "Using Notes" on page 132
- "Managing Mail Messages" on page 136
- "Managing Folders" on page 139
- "Using Address Books" on page 142
- "Using Rules" on page 146
- "Downloading Messages from Other Accounts" on page 149
- "Giving Users Proxy Access to Your Mailbox and Calendar" on page 151
- "Changing Password and Secret Question/Answer Information" on page 151
- "Changing WebAccess Settings" on page 152
- "Changing Time and Date Settings" on page 153

Starting and Exiting the WebAccess Interface

To start and log in to WebAccess:

1. Specify the URL for NetMail obtained from your administrator.
2. Specify your user name.

   The username (or User ID) is not case sensitive. For example, MargaretV is the same as margaretv.
3. Specify your password.

   The password is case sensitive. For example, AAGGHJKL is not the same as aagghjkl.
4. Click OK.

To exit and log out of WebAccess:

1 Click Exit  .

Use Exit to properly log out, rather than just closing your browser.

Viewing and Sending Mail Messages

The main function of the WebAccess mail system is to view and send e-mail messages.

This section covers the following messaging tasks:

- "Viewing Received and Sent Mail Messages" on page 115
- "Viewing and Saving Attachments" on page 115
- "Sending Mail Messages" on page 116
- "Sending Mail Messages with Attachments" on page 117
- "Adding and Removing a Signature on Outgoing Items" on page 117

Viewing Received and Sent Mail Messages

Received messages are messages that arrive in your mailbox. Sent messages are the messages that you send to other recipients. You can view both received and sent messages.

IMPORTANT: By default, copies of sent messages are not retained in your mailbox. Therefore, you must set up a folder for sent messages before you can view sent messages. For more information, see "Setting Up and Removing the Sent Folder" on page 142.

To view a received message:

1 From the Folder List, click INBOX.

2 From the INBOX item list, click the message you want to open.

The mail message appears in a separate window, allowing you to view, forward, reply to, move, delete, print, and change message options (read later, view the source, mark public/private, and set the message priority).

To view a sent message:

1 From the Folder List, select the folder you created for sent items.

2 From the Sent Folder item list, click the sent message you want to view.

Viewing and Saving Attachments

All WebAccess items you send or receive can include attachments of any file type (for example, text, audio, image, video, and application).

When you view an attached file, WebAccess attempts to convert the file to HTML and opens it in your browser. If WebAccess cannot convert the file, try opening the file within your browser. Depending on your browser configuration, you can expect the browser to display the file, launch an application to view the file in its native format, or save the file.

When NetMail sends a message, it encodes attachments in base64, which increases the size of the attachment 25 to 30 percent from the original file.

To view an attachment:

1 From the INBOX item list, click the message that contains the attachment you want to view.

2 Click attachment.

3 Click Open.

To save an attachment in its native format:

1 From the INBOX item list, click the message that contains the attachment you want to save.

2 Click attachment.

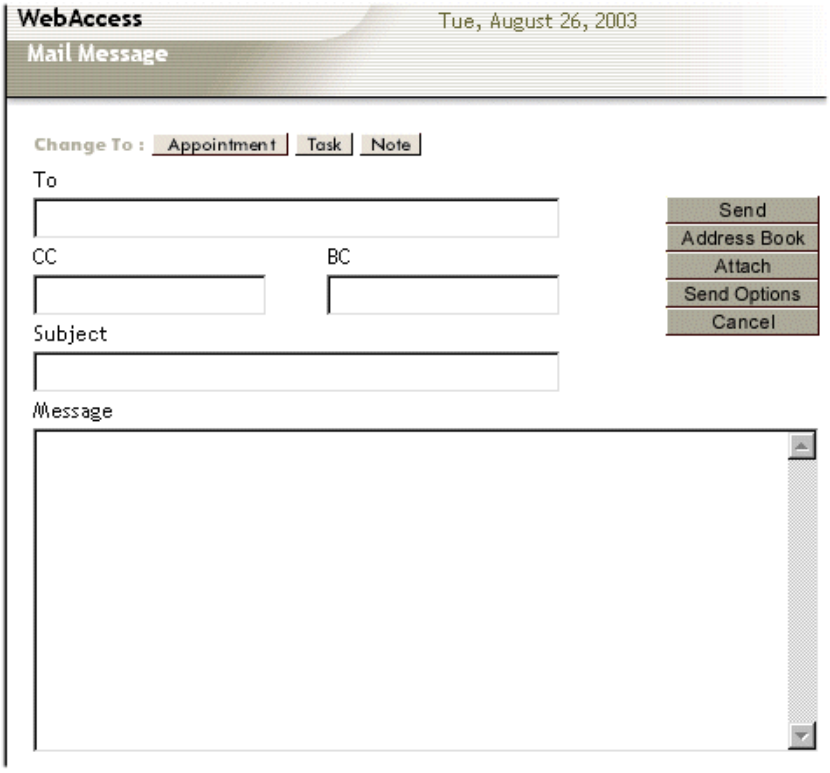
3 Click Save and browse to the location where you want to save the file.

4 Click Close.

The file is saved to the specified directory.

Sending Mail Messages

Description: Compose Mail Message window in WebAccess



To send a message

1 Click Compose .

2 Click Address Book to add recipients' e-mail addresses in the To, CC, and BC fields. When you are finished adding contacts, click Compose. For more information, see "Using Address Books" on page 142.

or

Type recipients' e-mail addresses, separated by a semicolon, a comma, or a space, in the To, CC, and BC fields.

3 Type a subject and message in the subject and Message fields.

4 Click Send Options to set the message priority and the delivery status notification.

For more information, see "Setting the Mail Message Priority" on page 137 and "Setting Delivery Status Notification" on page 138.

5 Click Send.

Sending Mail Messages with Attachments

All WebAccess items you send or receive can include attachments of any file type (for example, text, audio, images, video, and application files).

You can attach one or more files to an item to send to other users. For example, you might want to send a document in a mail message to another user.

When NetMail sends a message, it encodes attachments in base64, which increases the size of the attachment 25 to 30 percent from the original file.

To attach files to an item, your browser must support attachments.

To send a message with an attachment:

1 Click Compose  .

2 Click Address Book to add recipients' e-mail addresses in the To, CC, and BC fields. When you are finished adding contacts, click Compose. For more information, see "Using Address Books" on page 142.

or

Type recipients' e-mail addresses, separated by a semicolon, a comma, or a space, in the To, CC, and BC fields.

3 Type a subject and message in the subject and Message fields.

4 Click Attach.

5 For each file you want to attach, do the following:

5a Click Browse to locate the file you want to attach.

5b Click the file you want to attach, then click Open.

5c Click Add.

To remove any attachments, click the Remove option next to each attachment, then click OK.

6 Click OK when finished adding attachments.

7 Click Send Options to set the message priority and the delivery status notification.

For more information, see "Setting the Mail Message Priority" on page 137 and "Setting Delivery Status Notification" on page 138.

8 Click Send.

Adding and Removing a Signature on Outgoing Items

A signature provides contact information that is automatically included at the end of messages, appointments, tasks, and notes that you send.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Signature feature.

To add a signature to your outgoing messages:

1. Click Options > Mailbox Management.
2. Under Mailbox Settings, click Yes for the Add Signature to Outgoing Messages option.
3. In the Signature field, provide the information you want to appear at the bottom of each message you send.

   For example:

   Sam Marshall
   My Company
   Office of IT
   smarshal@mycompany.com
   405-423-7323
4. Click Save.

To remove a signature to your outgoing messages:

1. Click Options > Mailbox Management.
2. Under Mailbox Settings, click No for the Add Signature to Outgoing Messages option.
3. Click Save.

Forwarding Items

You can individually forward messages, appointments, tasks, and notes to another recipient or e-mail account or you can set up automatic forwarding to forward all incoming messages to another recipient or e-mail account.

NOTE: You can use the Rules feature to forward incoming messages to specific folders, recipients, or e-mail accounts under defined conditions. For more information, see "Using Rules" on page 146.

This section covers the following tasks:

- "Forwarding Mail Messages, Appointments, Tasks, and Notes" on page 118
- "Setting Up and Removing Automatic Forwarding" on page 119

Forwarding Mail Messages, Appointments, Tasks, and Notes

1. From the Item list, click the message to open it.
2. Click Forward .
3. Click Address Book to add recipients' e-mail addresses in the To, CC, and BC fields. When you are finished adding contacts, click Compose. For more information, see "Using Address Books" on page 142.

   or

   Type recipients' e-mail addresses, separated by a semicolon, a comma, or a space, in the To, CC, and BC fields.
4. Type an additional message in the Message field.
5. Click Send.

Setting Up and Removing Automatic Forwarding

You can use the Automatic Forwarding feature to automatically forward all incoming messages to a recipient or e-mail account.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Automatic Forwarding feature.

To set up automatic forwarding:

1. Click Options > Mailbox Management.
2. Under Mailbox Settings, select Yes for the Forward All New Messages option.
3. If you want to keep copies of your messages in your mailbox, select Yes for the Keep Copy option.

   IMPORTANT: If you select No for this option, the forwarded messages no longer appear in the WebAccess account.
4. Type one or more e-mail addresses in the Forward To field.

   Use Return to move to the next line and list one e-mail address per line.
5. Click Save.

To remove automatic forwarding:

1. Click Options > Mailbox Management.
2. Under Mailbox Settings, select No for the Automatically Forward to All New Messages option.
3. Click Save.

Replying to Items

When you receive items, you can send a reply message directly to the original sender of the message or you can reply to all the recipients included on the original message.

You can also set up and remove an automatic reply to the sender or original recipients.

NOTE: You can use the Rules feature to automatically respond to specific messages under defined conditions. For more information, see "Using Rules" on page 146.

This section covers the following tasks:

- "Replying to Received Mail Messages, Appointments, Tasks, and Notes" on page 119
- "Setting Up and Removing an Automatic Reply" on page 120
- "Providing a Different Address for a Reply" on page 120

Replying to Received Mail Messages, Appointments, Tasks, and Notes

In addition to accepting or declining an appointment, task, or note, you can also send a reply message to the original sender or to all message recipients.

To reply to messages, appointments, tasks, and notes:

1. From the Item list, click the item to open it.
2. Click Reply to Sender or Reply to All.

Reply to Sender sends your response to the original sender. Reply to All sends your response to the original sender and everyone that was included as a recipient on the original message.

3. Type an additional message in the Message field.
4. Click Send.

Setting Up and Removing an Automatic Reply

When you are unavailable and you cannot retrieve your messages for an extended period of time (such as when you are away at a conference, vacation, or tied up in meetings), you can set up an automatic reply with a message. When you return, immediately remove your automatic reply.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Automatic Reply feature.

To set up an automatic reply:

1. Click Options > Mailbox Management.
2. Under Mailbox Settings, select Yes for the Automatically Reply to All New Messages option.
3. Type the message you want to include in your automatic reply. For example:

   ```
   I am on vacation from April 1 to April 15. If you need anything during
   that time, please contact Brian Thompson at bthompson@mycompany.com.
   ```

4. Click Save.

To remove an automatic reply:

1. Click Options > Mailbox Management.
2. Under Mailbox Settings, select No for the Automatically Reply to All New Messages option.
3. Click Save.

Providing a Different Address for a Reply

If you do not want recipients to reply to a message you send to your current mailbox, you can specify a different e-mail address that the system automatically uses when recipients reply to your messages.

For example, if you use your account for a customer survey, you might want the survey respondents to return their responses to another e-mail address so they do not contact you directly

NOTE: Depending on how your administrator has configured your system, you might not have access to the Reply To Address feature.

To configure your Reply To address:

1. Click Options > General Settings.
2. Under WebAccess Settings, specify your preferred Reply To e-mail address in the Reply To field.

   IMPORTANT: Specifying a different address for a reply does not automatically enable you to receive mail at that address. You must provide an existing Internet e-mail address, such as jason@mywebaccess.com.

3. Click Save.

   Now when you send a message and the recipient replies, the reply message is automatically addressed to the specified Reply To address.

To remove your Reply To address:

1. Click Options  > General Settings.
2. Under WebAccess Settings, remove your preferred Reply To e-mail address in the Reply To field.
3. Click Save.

Scheduling Appointments and Using the Calendar

The calendar lets you view appointments, tasks, or notes you receive from others or create to send to yourself. Using the calendar, you can view your schedule one day, one week, or one month at a time.

When accepted, the calendar displays all appointments, tasks, and notes you receive. From your calendar, you can also schedule appointments, assign tasks, and write notes to other users.

This section covers the following calendar tasks:

- "Changing the Time Span of the Calendar View" on page 121
- "Scheduling Appointments" on page 122
- "Using Busy Search for People and Resources" on page 124
- "Accepting, Declining, and Delegating Appointments" on page 125
- "Using Multiple Calendars" on page 125
- "Marking Appointments Unread (Read Later)" on page 126
- "Moving and Copying Appointments to Folders and Other Calendars" on page 127
- "Deleting and Undeleting Appointments" on page 127

NOTE: Depending on how your administrator has configured your system, you might not have access to the calendaring features.

Changing the Time Span of the Calendar View

Using the calendar, you can view your schedule one day, one week, or one month at a time. You can also change the year that you want to view.

To change the day:

1. Click Calendar  .
2. Click Day.
3. In Calendar, select the day you want to view.

   or

   From the Day drop-down list, click the day you want to view, then click Change To.

   or

   Click Today to change the calendar view to the current day.

To change the week:

1. Click Calendar  .
2. Click Week.

3 From the Day drop-down list, click a day in the week you want to view, then click Change To.

or

Click Today to change the calendar view to the current week.

To change the month:

1 Click Calendar  > Month

2 In the calendar, click the right and left arrows by the month to select the month you want to view.

or

From the Month drop-down list, click the month you want to view, then click Change To.

To change the year:

1 Click Calendar  .

2 In the calendar, continue to click the right and left arrows by the month to select the year you want to view.

or

From the Year drop-down list, click the year you want to view, then click Change To.

Scheduling Appointments

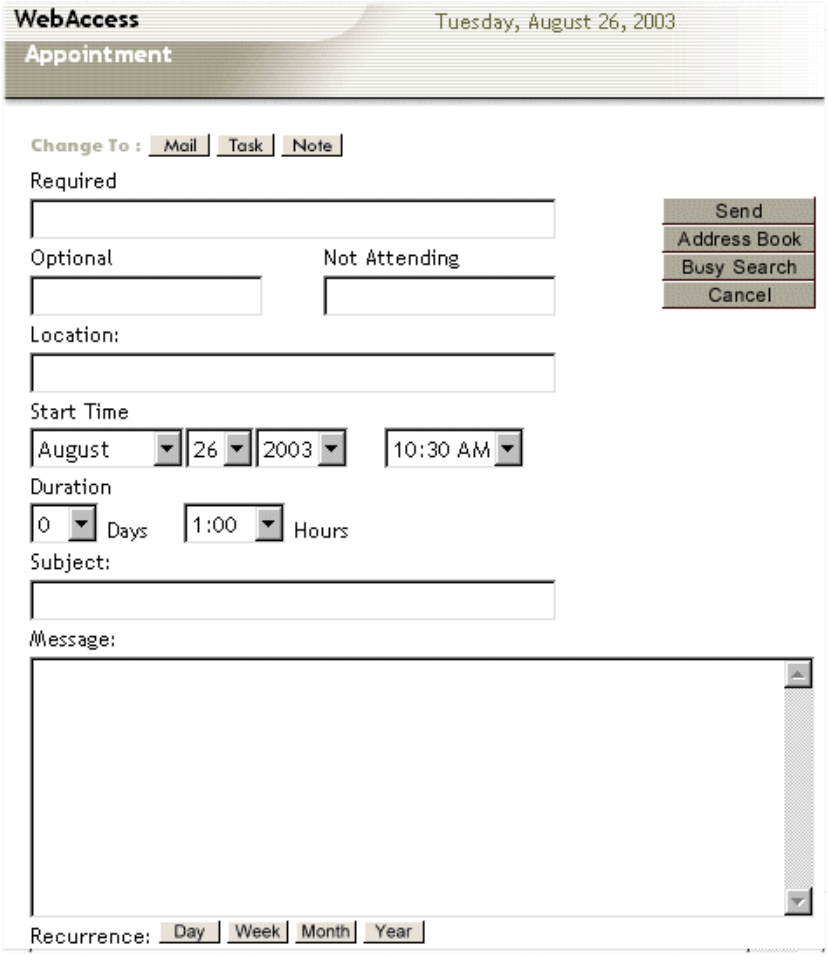
Using the Appointment feature, you can schedule appointments, people, and resources.

The Busy Search feature allows you to check people's schedules and resource availability to determine the best time to schedule an appointment. For more information on the Busy Search feature, see "Using Busy Search for People and Resources" on page 124.

When you set up appointments, you can address recipients in Required, Optional, and Not Attending fields to indicate to recipients your intent and expectations in inviting them to the appointment. Recipients can then accept, decline, or delegate the appointment.

Use the Required field to schedule resources.

Description: Compose Appointment window in WebAccess



To schedule an appointment:

1. Click Compose > Appointment.

   or

   Click Calendar > Appointment.

2. Click Address Book to add recipients' and resources' e-mail addresses in the Required, Optional, or Not Attending fields. When you are finished adding contacts and resources, click Compose. For more information, see "Using Address Books" on page 142.

   or

   Type recipents' and resources' e-mail addresses, separated by a semicolon, a comma, or a space, in the Required, Optional, or Not Attending fields.

   or

   Leave all the recipient fields blank to create a personal appointment that appears only in your calendar.

3. Specify a location for the appointment.

   The Location field is only a text field, which allows you to provide a description of the location. However, to actually schedule a resource, you must specify the resource in the Required field.

4 Use the Start Time drop-down lists to specify a month, a day, year, and beginning time for the appointment.

5 Use the Duration drop-down lists to specify the number of days or hours.

6 Type a subject and message for the appointment in the Subject and Message fields.

7 If the appointment occurs on a regular basis, specify the recurrence settings. Click Day, Week, Month, and Year as appropriate.

The maximum value you can provide for number of occurrences for recurring events daily, weekly, monthly, and yearly is 100.

7a Specify the appropriate number of days, weeks, months, or years before you want the appointment to reappear in the recipients' mailboxes.

7b Select one of the following options:

- No End Date.
- End after *x* occurrences, where *x* indicates the number of occurrences.
- End by Month, Day, Year, and Time. Use the drop-down lists to specify each one.

8 Click Send.

Using Busy Search for People and Resources

You can use busy search to find out when people and resources (such as conference rooms) are available. It simplifies setting up appointments and saves times in scheduling with others.

To use busy search for scheduling people and resources:

1 Click Compose  > Appointment.

or

Click Calendar  > Appointment.

2 Click Address Book to add recipients' and resources' e-mail addresses in the Required, Optional, or Not Attending fields. When you are finished adding contacts and resources, click Compose. For more information, see "Using Address Books" on page 142.

or

Type recipients' and resources' e-mail addresses separated by a semicolon, a comma, or a space, in the Required, Optional, or Not Attending fields.

or

Leave all the recipient fields blank to create a personal appointment that appears only in your calendar.

3 Specify a location for the appointment.

The Location field is only a text field, which allows you to provide a description of the location. However, to actually schedule a resource, you must specify the resource in the Required field.

4 Use the Start Time drop-down lists to specify a month, a day, year, and beginning time for the appointment.

5 Use the Duration drop-down lists to specify the number of days or hours.

6 Type a subject and message for the appointment in the Subject and Message fields.

7 Click Busy Search to find out what time participants and the conference room have free time or busy time.

If a critical participant is busy, click Cancel and reset the time. Then perform the busy search again if needed.

8 Click Send.

Accepting, Declining, and Delegating Appointments

When you receive an appointment invite, you can either accept it, decline it, or delegate it.

To accept an appointment:

1 Click Mailbox  .

2 Click the check box to the left of the appointment you want to accept, then click Accept.

or

Click the appointment to open it, then click Accept  .

The appointment is deleted (not purged) from the INBOX item list and appears on your calendar.

To decline an appointment:

1 Click Mailbox  (if the appointment is not already accepted).

or

Click Calendar  > the date of appointment you want to decline.

2 Click the check box to the left of the appointment you want to decline, then click Decline.

or

Click the appointment to open it, then click Decline  .

The appointment is deleted (not purged) from your mailbox.

To delegate an appointment:

1 Click Mailbox  (if the appointment is not already accepted).

or

Click Calendar  > the date of appointment you want to delegate.

2 Click the appointment to open it > Delegate  .

3 Type the e-mail address of the person to whom you want to delegate the appointment, then add any comments in the Comment to Delegatee field.

4 Click Send.

The appointment is deleted (not purged) from your mailbox and sent to the delegatee you specified.

Using Multiple Calendars

WebAccess gives you the benefits and capabilities of working with multiple calendars.

For example, you can maintain your own personal calendar, a general calendar for your organization, or calendars for various resources.

With multiple calendars, you can move or copy appointments, tasks, and notes between calendars.

NOTE: You can use the Rules feature to accept and move incoming appointments, notes, and tasks to a different calendar under defined conditions. For more information, see "Using Rules" on page 146.

To add multiple calendars to your account:

1. From the Folder List, click Add Folder.
2. In the Folder Name field, specify the name of your calendar.
3. Select Calendar as the type of folder you want to add.
4. Click the folder where you want to create the calendar.

   By default, new folders are added at the root level of the mailbox.
5. Click OK.

To move items between calendars:

1. From the Folder List, select the calendar that contains the item you want to move.
2. Within the calendar, locate the item you want to move.
3. Click the check box to the left of the item you want to move.

   or

   Click the item to open it, then click Move  .
4. Select the calendar where you want to move the item.
5. Click OK.

To copy items between calendars:

1. From the Folder List, select the calendar that contains the item you want to copy.
2. Within the calendar, locate the item you want to copy.
3. Click the check box to the left of the item you want to copy.
4. Select the calendar where you want to copy the item.
5. Click OK.

Marking Appointments Unread (Read Later)

You can mark an appointment to appear as if it is unopened or unread. For example, if you opened an appointment and are interrupted, you might want to mark the appointment as unread to remind you to read it later.

To mark an appointment unread:

1. From the INBOX item list, click the check box to the left of the appointment you want to mark as unread, then click Read Later.

   or

   From the INBOX item list, click the appointment to open it, click Message Options  , then click Read Later  .

   The appointment is marked as unread.

Moving and Copying Appointments to Folders and Other Calendars

If the appointment is not accepted, you can move it to another folder. When you accept it, it is deleted (not purged) from the INBOX item list and appears on your calendar. You can move or copy the accepted appointment from one calendar to another.

NOTE: You can use the Rules feature to accept and move incoming appointments, notes, and tasks to a different calendar under defined conditions. For more information, see "Using Rules" on page 146.

To move an appointment to another folder:

1. Locate the appointment you want to move from the INBOX item list.
2. Click the check box to the left of the appointment you want to move.

   or

   Click the appointment to open it, then click Move  .
3. Select the folder where you want to move the appointment.
4. Click OK.

   The appointment is moved to the specified folder.

To copy an appointment to another folder:

1. Locate the appointment you want to copy from the INBOX item list.
2. Click the check box to the left of the appointment you want to copy.
3. Select the folder where you want to copy the appointment.
4. Click OK.

   The appointment is copied to the specified folder.

To move an accepted appointment to another calendar:

1. In your calendar, locate the appointment you want to move.
2. Click the check box to the left of the appointment you want to move, then click Move.
3. Select the calendar where you want to move the appointment.
4. Click OK.

   The appointment is moved to the specified calendar.

To copy an accepted appointment to another calendar:

1. In your calendar, locate the appointment you want to copy.
2. Click the check box to the left of the appointment you want to move, then click Copy.
3. Select the calendar where you want to copy the appointment.
4. Click OK.

   The appointment is copied to the specified calendar.

Deleting and Undeleting Appointments

When appointments are deleted from the calendar, they are automatically purged.

IMPORTANT: Use care in deleting already accepted appointments, tasks, and notes. When these items are deleted, you cannot undelete them. The only time that you can undelete an appointment, task, or note, is if it still exists as a deleted item in the INBOX item list.

To delete an appointment:

1. Locate the appointment you want to delete from the INBOX item list.
2. Click the check box to the left of the appointment you want to delete, then click Delete.

   or

   Click the appointment to open it, then click Delete  .

To undelete an appointment from the INBOX item list or folder:

1. Locate the appointment you want to undelete from the INBOX item list or folder.
2. Click the check box to the left of the appointment you want to undelete, then click Undelete.

Using Tasks

This section covers the following tasks:

- "Viewing Tasks" on page 128
- "Assigning Tasks" on page 128
- "Accepting, Declining, and Delegating Tasks" on page 130
- "Marking Tasks Completed" on page 131
- "Marking Tasks Unread (Read Later)" on page 131
- "Moving and Copying Tasks to Folders and Other Calendars" on page 131
- "Deleting and Undeleting Tasks" on page 132

Viewing Tasks

You can view a task from the mailbox (before accepting or declining it) or calendar. Declined tasks are deleted (not purged) from your mailbox.

To view a received task:

1. Locate the task you want to open either from the INBOX item list or calendar, depending upon whether the task is accepted.
2. From the INBOX item list, click the task you want to open.

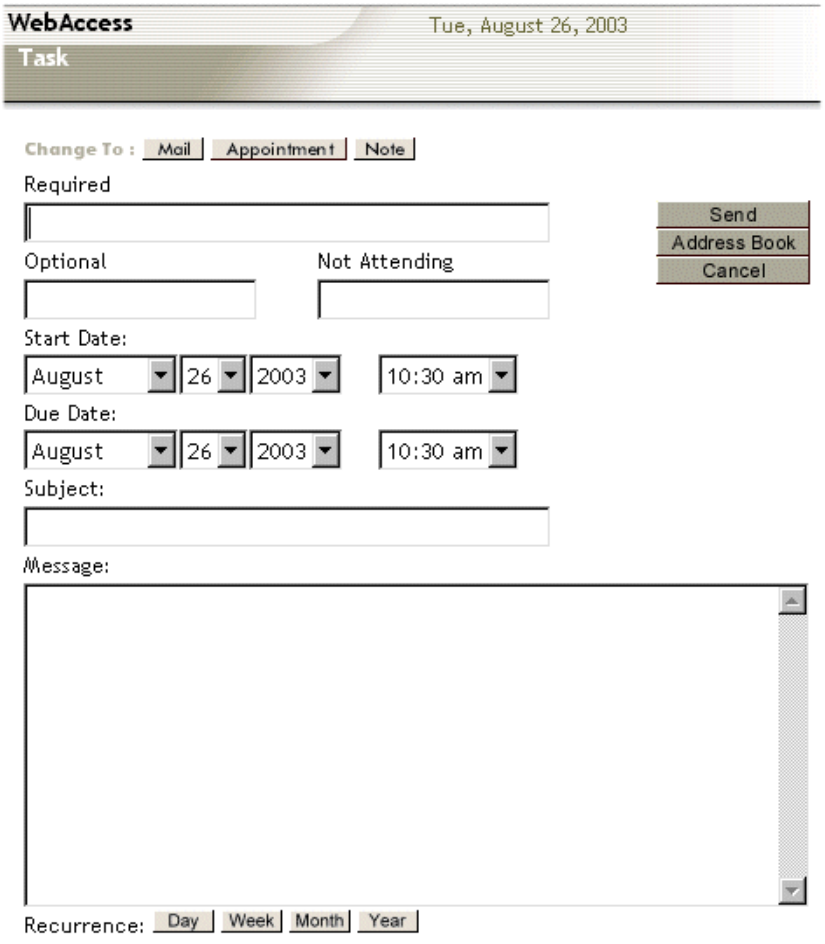
   The task appears in a separate window, allowing you to view, accept, decline, delegate, forward, reply to, move, delete, change message options, and print.

Assigning Tasks

You can send tasks to yourself and others that appear on your personal calendar and other recipients' calendars. Recipients can choose to either accept, decline, or delegate a task.

When you assign tasks, you can address recipients in Required, Optional, and Not Attending fields to indicate to recipients your intent and expectations in assigning the task.

Description: Compose Task window in WebAccess



To assign a task:

1. Click Compose > Task.

   or

   Click Calendar > Task.

2. Click Address Book to add recipients' e-mail addresses in the Required, Optional, or Not Attending fields. When you are finished adding contacts, click Compose. For more information, see "Using Address Books" on page 142.

   or

   Type recipients' e-mail addresses, separated by a semicolon, a comma, or a space, in the Required, Optional, or Not Attending fields.

   or

   Leave all the recipient fields blank to create a personal task that appears only in your calendar.

3. Use the Start Date drop-down lists to specify a month, a day, year, and time that you want the task to appear on the recipient's calendar.

4. Use the Due Date drop-down lists to specify a month, a day, year, and time when you want the task completed.

5. Type a subject for the task in the Subject field.

6 Type the instructions or task description in the Message field.

7 Click Day, Week, Month, and Year as appropriate to set up a task recurrence.

7a Specify the appropriate number of days, weeks, months, or years before you want the task to reappear in the recipients' mailboxes.

7b Select one of the following options:

- No End Date.
- End after *x* occurrences, where *x* indicates the number of occurrences.
- End by Month, Day, Year, and Time. Use the drop-down lists to specify each one.

8 Click Send.

Accepting, Declining, and Delegating Tasks

When you receive a task, you can accept, decline, or delegate it.

To accept a task:

1 Click Mailbox  .

2 Click the check box to the left of the task you want to accept, then click Accept.

or

Click the task to open it, then click Accept  .

The task is deleted (not purged) from the INBOX item list and appears on your calendar.

To decline a task:

1 Click Mailbox  (if the task is not already accepted).

or

Click Calendar  > the date of task you want to decline.

2 Click the check box to the left of the task you want to decline, then click Decline.

or

Click the task to open it, then click Decline  .

The task is deleted (not purged) from your mailbox.

To delegate a task:

1 Click Mailbox  (if the task is not already accepted).

or

Click Calendar  > the date of task you want to delegate.

2 Click the task to open it > Delegate  .

3 Type the e-mail address of the person to whom you want to delegate the task, then add any comments in the Comment to Delegatee field.

4 Click Send.

The task is deleted (not purged) from your mailbox and sent to the delegatee you specified.

Marking Tasks Completed

When you complete a task, you can mark it completed to remove it from your mailbox.

1. Click Calendar > the date of the task.
2. Click the check box to the left of the task you want to mark as complete, then click Complete.

   or

   Click the task to open it, then click Complete .

Marking Tasks Unread (Read Later)

You can mark a task to appear as if it is unopened or unread. For example, if you opened a task and are interrupted, you might want to mark the task as unread to remind you to read it later.

1. From the INBOX item list, click the check box to the left of the task you want to mark as unread, then click Read Later.

   or

   From the INBOX item list, click the task to open it, click Message Options , then click Read Later .

   The task is marked as unread.

Moving and Copying Tasks to Folders and Other Calendars

If the task is not accepted, you can move it to another folder. When you accept it, it appears only in the calendar. You can move or copy the accepted task from one calendar to another.

NOTE: You can use the Rules feature to accept and move incoming appointments, notes, and tasks to a different calendar under defined conditions. For more information, see "Using Rules" on page 146.

To move a task to another folder:

1. Locate the task you want to move from the INBOX item list.
2. Click the check box to the left of the task you want to move.

   or

   Click the task to open it, then click Move .
3. Select the folder where you want to move the task.
4. Click OK.

   The task is moved to the specified folder.

To copy a task to another folder:

1. Locate the task you want to copy from the INBOX item list.
2. Click the check box to the left of the task you want to copy.
3. Select the folder where you want to copy the task.
4. Click OK.

   The task is copied to the specified folder.

To move a accepted task to another calendar:

1. In your calendar, locate the task you want to move.

2 Click the check box to the left of the task you want to move, then click Move.

3 Select the calendar where you want to move the task.

4 Click OK.

The task is moved to the specified calendar.

To copy a accepted task to another calendar:

1 In your calendar, locate the task you want to copy.

2 Click the check box to the left of the task you want to move, then click Copy.

3 Select the calendar where you want to copy the task.

4 Click OK.

The task is copied to the specified calendar.

Deleting and Undeleting Tasks

When tasks are deleted from the calendar, they are automatically purged.

IMPORTANT: Use care in deleting already accepted appointments, tasks, and notes. When these items are deleted, you cannot undelete them. The only time that you can undelete an appointment, task, or note, is if it still exists as a deleted item in the INBOX item list.

To delete a task:

1 Locate the task you want to delete from the INBOX item list.

2 Click the check box to the left of the task you want to delete, then click Delete.

or

Click the task to open it, then click Delete  .

To undelete a task from the INBOX item list or folder:

1 Locate the task you want to undelete from the INBOX item list or folder.

2 Click the check box to the left of the task you want to undelete, then click Undelete.

Using Notes

Notes allow you to indicate the day you want the note to appear on the recipient's calendar. Because notes are posted in the recipient's calendar, you can use them as reminders of specific events, such as days off, project deadlines, or birthdays.

This section covers the following tasks:

- "Viewing Notes" on page 133
- "Writing Notes" on page 133
- "Accepting, Declining, and Delegating Notes" on page 134
- "Marking Notes Unread (Read Later)" on page 135
- "Moving and Copying Notes to Folders and Other Calendars" on page 135
- "Deleting and Undeleting Notes" on page 136

Viewing Notes

You can view a note from the INBOX item list (before accepting or declining it) and from the calendar. Declined notes are deleted (not purged) from your mailbox.

1. Click Mailbox (if the note is not already accepted).

   or

   Click Calendar > the date of note you want to view.

2. Click the note you want to open.

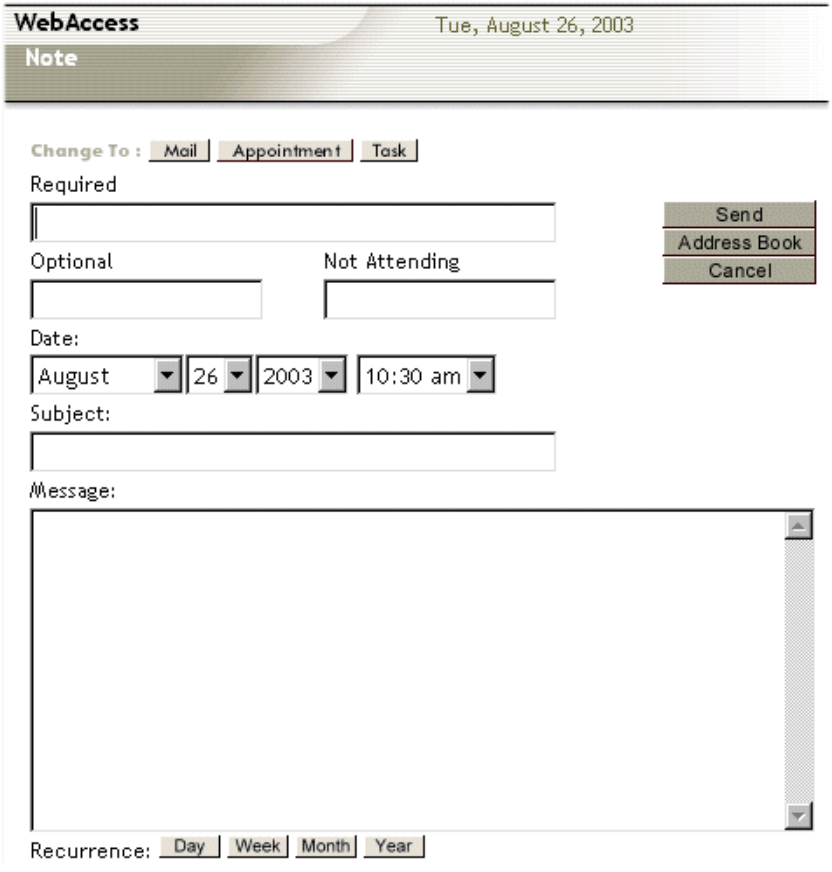
   The note appears in a separate window, allowing you to view, accept, decline, delegate, forward, reply to, move, delete, change message options, and print.

Writing Notes

You can write notes that you want to appear on your personal calendar and other recipients' calendars. Because notes are posted in the recipient's calendar, you can use them as reminders of specific events, such as days off, project deadlines, or birthdays.

When you write notes, you can address recipients in Required, Optional, and Not Attending fields to indicate to recipients your intent and expectations in writing the note.

Description: Compose Note window in WebAccess



To write a note:

1. Click Compose > Note.

or

Click Calendar  > Note.

2 Click Address Book to add recipients' e-mail addresses in the Required, Optional, or Not Attending fields. When you are finished adding contacts, click Compose. For more information, see "Using Address Books" on page 142.

or

Type recipients' e-mail addresses, separated by a semicolon, a comma, or a space, in the Required, Optional, or Not Attending fields.

or

Leave all the recipient fields blank to create a personal note that appears only in your calendar.

3 Use the Date drop-down list to specify a month, a day, year, and time for the note to appear on recipients' calendars.

4 Type a subject and message for the note in the Subject and Message fields.

5 If you want the note to occur on a regular basis, specify the recurrence settings. Click Day, Week, Month, and Year as appropriate.

5a Specify the appropriate number of days, weeks, months, or years before you want the note to reappear in recipients' calendars.

5b Select an option.

- No End Date.
- End after *x* occurrences, where *x* indicates the number of occurrences.
- End by Month, Day, Year, and Time. Use the drop-down lists to specify each one.

6 Click Send.

Accepting, Declining, and Delegating Notes

When you receive a note, you can either accept it, decline it, or delegate it. Accepted notes appear on the calendar and no longer appear in the INBOX item list. Declined notes are deleted (not purged) from the mailbox.

To accept a note:

1 Click Mailbox  .

2 Click the check box to the left of the note you want to accept, then click Accept.

or

Click the note to open it, then click Accept  .

The note is deleted (not purged) from the INBOX item list and appears on your calendar.

To decline a note:

1 Click Mailbox  (if the note is not already accepted).

or

Click Calendar  > the date of note you want to decline.

2 Click the check box to the left of the note you want to decline, then click Decline.

or

Click the note to open it, then click Decline  .

The note is deleted (not purged) from the INBOX item list and calendar.

To delegate a note:

1. Click Mailbox  (if the note is not already accepted).

   or

   Click Calendar  > the date of task you want to delegate.
2. Click the note to open it, then click Delegate  .
3. Type the e-mail address of the person to whom you want to delegate the note, then add any comments in the Comment to Delegatee field.
4. Click Send.

   The note is deleted (not purged) from your mailbox and sent to the delegatee you specified.

Marking Notes Unread (Read Later)

You can mark a note to appear as if it is unopened or unread. For example, if you opened a note and are interrupted, you might want to mark the note as unread to remind you to read it later.

1. From the INBOX item list, click the check box to the left of the note you want to mark as unread, then click Read Later.

   or

   From the INBOX item list, click the note to open it, click Message Options  , then click Read Later  .

   The note is marked as unread.

Moving and Copying Notes to Folders and Other Calendars

If the note is not accepted, you can move it to another folder. When you accept it, it appears only in the calendar and no longer in the INBOX item list. You can move or copy the accepted note from one calendar to another.

NOTE: You can use the Rules feature to accept and move incoming appointments, notes, and tasks to a different calendar under defined conditions. For more information, see "Using Rules" on page 146.

To move a note to another folder:

1. Locate the note you want to move from the INBOX item list.
2. Click the check box to the left of the note you want to move.

   or

   Click the note to open it, then click Move  .
3. Select the folder where you want to move the note.
4. Click OK.

   The note is moved to the specified folder.

To copy a note to another folder:

1. Locate the note you want to copy from the INBOX item list.

2. Click the check box to the left of the note you want to copy.
3. Select the folder where you want to copy the note.
4. Click OK.

   The note is copied to the specified folder.

To move a accepted note to another calendar:

1. In your calendar, locate the note you want to move.
2. Click the check box to the left of the note you want to move, then click Move.
3. Select the calendar where you want to move the note.
4. Click OK.

   The note is moved to the specified calendar.

To copy a accepted note to another calendar:

1. In your calendar, locate the note you want to copy.
2. Click the check box to the left of the note you want to move, then click Copy.
3. Select the calendar where you want to copy the note.
4. Click OK.

   The note is copied to the specified calendar.

Deleting and Undeleting Notes

When notes are deleted from the calendar, they are automatically purged.

IMPORTANT: Use care in deleting already accepted appointments, tasks, and notes. When these items are deleted, you cannot undelete them. The only time that you can undelete an appointment, task, or note, is if it still exists as a deleted item in the INBOX item list.

To delete a note:

1. Locate the note you want to delete from the INBOX item list.
2. Click the check box to the left of the note you want to delete, then click Delete.

   or

   Click the note to open it, then click Delete  .

To undelete a note from the INBOX item list or folder:

1. Locate the note you want to undelete from the INBOX item list or folder.
2. Click the check box to the left of the note you want to undelete, then click Undelete.

Managing Mail Messages

This section covers the following tasks:

- "Setting the Mail Message Priority" on page 137
- "Marking a Message As Public or Private" on page 137
- "Marking Mail Messages Unread (Read Later)" on page 138
- "Setting Delivery Status Notification" on page 138

- "Moving and Copying Mail Messages to Folders" on page 138
- "Deleting and Undeleting Mail Messages" on page 139
- "Enabling and Disabling Immediate Purge of Deleted Mail Messages" on page 139

Setting the Mail Message Priority

When sending a mail message or when viewing a received mail message, appointment, task, or note, you can set or reset the priority on the item.

You can select High, Normal, or Low, indicating the importance level of the message.

NOTE: When sending a message, you cannot set a priority on appointments, tasks, or notes.

To set the message priority when sending a mail message:

1. Click Compose  .
2. In the Message Compose window, click Send Options.
3. Under Priority, select either High, Normal, or Low.
4. Click OK.
5. When you are finished writing your mail messages, click Send.

To set the message priority for personal copy on a received mail message, appointment, task, or note:

1. Click the item you want to change to open it.
2. Click Message Options  .
3. Click High  , Normal  ,or Low  .
4. Click OK.

Marking a Message As Public or Private

(0October 7, 2003- Not on interface) New icon to show how a file is marked (public or private) is under discussion.

When viewing a received mail message, appointment, task, or note, you can mark the item as Public or Private. Marking a message as Public allows those you specify to share your message folder to view the message. Marking a message as Private prevents anyone from viewing the item (including those with shared access) except the mailbox owner.

NOTE: The ability to mark a message public or private works in both private and shared folders. When you mark a message in a shared folder as private, it is the same as moving the message to a private folder. The only one who can access it is the mailbox owner

To mark a received mail message, appointment, task, or note as public or private:

1. Click the item for which you want to change the status to open it.
2. Click Message Options  > Public  or Private  .
3. Close the message.

Marking Mail Messages Unread (Read Later)

You can mark a message to appear as if it is unopened for unread. For example, if you opened a message and are interrupted, you might want to mark the message as unread to remind you to read it later.

1. From the INBOX item list, click the check box to the left of the mail message you want to mark as unread, then click Read Later.

   or

   From the INBOX item list, click the mail message to open it, click Message Options  , then click Read Later  .

   The mail message is marked as unread.

Setting Delivery Status Notification

Delivery Status Notification notifies you upon successful or failed delivery.

1. Before sending a message, click Send Options.
2. Under Delivery Status Notification, select one of the following options:
   - **Failure**. Notifies you when a message failed. By default, Failure is selected.
   - **Success**. Notifies you when the message is successfully delivered.
   - **Failure and Success**. Allows you to receive a notification of failure or success as available in the previous options.
3. Click OK.

Moving and Copying Mail Messages to Folders

You can move or copy mail messages to other folders as needed.

NOTE: You can use the Rules feature to move incoming mail messages to a different folder under defined conditions. For more information, see "Using Rules" on page 146.

To move mail messages to other folders:

1. Locate the message you want to move.
2. Click the check box to the left of the message you want to move, then click Move.

   or

   Click a mail message to open it, then click Move  .
3. Click the folder where you want to move the message.
4. Click OK.

   The message is moved to the specified folder.

To copy mail messages to other folders.

1. Locate the message you want to copy.
2. Click the check box to the left of the message you want to copy, then click Copy.
3. Click the folder where you want to copy the message.
4. Click OK.

   The message is copied to the specified folder.

Deleting and Undeleting Mail Messages

When mail messages are deleted, the Delete mark ✕ is placed next to the mail messages to indicate it is deleted. The item is not permanently removed from your mailbox, however, until you purge it. As long as an item is not purged, you can still undelete it.

When the message is undeleted, the Delete mark ✕ is removed to indicate it is no longer deleted.

To delete a mail message:

1. Locate the message you want to delete.
2. Click the check box to the left of the message you want to delete, then click Delete.

   or

   Click the message to open it, then click Delete  .

To undelete a mail message from the INBOX item list or folder:

1. Locate the mail message you want to undelete from the INBOX item list or folder.
2. Click the check box to the left of the mail message you want to undelete, then click Undelete.

Enabling and Disabling Immediate Purge of Deleted Mail Messages

After you delete a mail message, it is not removed from your mailbox until you purge it. You can set up an immediate purge of deleted messages so you do not need to manually purge mail messages.

NOTE: Appointments, tasks, and notes are automatically purged upon delete.

To enable an immediate purge of deleted messages:

1. Click Options  > Mailbox Management.
2. Under Mailbox Settings, select Yes for the Immediate Purge of Deleted Messages option.
3. Click Save.

To disable an immediate purge of deleted messages:

1. Click Options  > Mailbox Management.
2. Under Mailbox Settings, select No for the Immediate Purge of Deleted Messages option.
3. Click Save.

Managing Folders

WebAccess provides folders to help organize the items you send and receive. The Folder List lets you select the folder you want open. The contents of the currently opened folder are displayed in the item list.

By default, the only folder in the Folder List is INBOX, where messages are stored when you first receive them.

You can add additional folders to further organize your items. For example, you can add a folder to store all messages you receive regarding a specific project you are working on.

This section covers the following tasks:

- “Adding Mailbox or Calendar Folders” on page 140

- "Hiding Folders" on page 140
- "Renaming Folders" on page 140
- "Working with Shared Folders and Calendars" on page 140
- "Setting Up and Removing the Sent Folder" on page 142
- "Deleting Folders" on page 142

Adding Mailbox or Calendar Folders

You can add new mailbox folders or calendar folders as needed to your mailbox.

1. From the Folder List, click Add Folder.
2. Type the folder name.
3. Select the type of folder you want to add: Mailbox or Calendar.
4. Select the folder where you want to add a new folder.

   For example, to add a folder inside the INBOX folder, select INBOX. By default, new folders are added at the root level of the mailbox.
5. Click OK.

Hiding Folders

To hide local folders from view or from proxy users:

1. Click Options  > Shared Folders.
2. Under Available Folders, click the check box next to the folder that you want to hide.
3. Click Save.
4. Click Exit  and log in again to WebAccess.

Renaming Folders

You can rename folders as needed.

1. From the Folder List, select Rename Folder.
2. Select the folder you want to rename.
3. Type a new name for the folder in the New Name field.
4. Click OK.

   When you look at the Folder List, the name is changed to the new folder name.

Working with Shared Folders and Calendars

A shared folder is like any other folder, except other people (subscribers) have access to it. For example, if you want to have a place where everyone in your department can store and view items like mail messages, documents, and so forth, you can share a folder. You can create shared folders or share existing personal folders. You choose whom to share the folder with, and what rights to grant each person.

Using shared folders, you can collaborate with team members to easily share all project information and correspondence. One advantage is when new members join the team and are given

rights to the team's shared folder; they immediately have all correspondence and background information available for the project.

When subscribers view the contents of the shared folder, they are viewing a local copy. When the shared folder is created, it replicates a copy of the master and copies it to subscribers' local clients. This allows the subscribers to mark and keep track of the items they have read.

When you place a document in a shared folder, subscribers with rights to view the contents of the shared folder do not automatically have rights to edit or add documents. Before they can edit or add documents, the owner of the document has to give them rights.

Four levels of rights exist:

- **Mark Read.** Allows you to mark the item (on your local copy) as read to help you keep track of opened items.
- **Read.** Allows you to open and view the local copy of the item.
- **Insert.** Allows you to copy an item to the shared folder, which puts the item into the master mailbox. The master mailbox then replicates the item and copies it to the local copy of the shared folder of those with rights to the folder.
- **Delete.** Allows you to delete and purge items from your local copy of the shared folder. The owner of the master mailbox can delete items within the master mailbox, but the delete is not replicated to the local mailboxes. Each individual user must manually delete outdated items.

Shared folders work with IMAP clients, including GroupWise, Ximian Evolution, Microsoft Outlook Express, Microsoft Outlook, Eudora, and Mulberry.

You can also use other features to benefit your team with shared folders. You can set up a personal group in your personal address book that contains all the e-mail addresses for the team members. For more information on the personal groups feature, see "Creating Personal Groups" on page 145.

In addition, you can set up a rule to add any correspondence to the Personal Group to the shared folder. For more information on the rules features, see "Using Rules" on page 146.

To share a folder or calendar with a subscriber:

1. Click Options > Shared Folders.
2. Under Add a Share, select the folder or calendar you want to share.
3. Under Add Share for User, type the user names (separated by a semicolon, comma, or space) that you want to give rights to share the folder.
4. Click Save.

To unsubscribe a remote folder from sharing:

1. Click Options > Shared Folders.
2. Under Folders you are sharing, click Delete next to any user that has rights to view the folder you do not want to share.
3. Click Save.

To grant or remove rights:

1. Click Options > Shared Folders.
2. Under Folders you are sharing, find the user or users you want to grant or remove rights.

3. Click in the Mark Read, Read, Insert, or Delete check boxes to select or deselect rights for users.
4. Click Save.

To remove user from access to shared folders or calendars:

1. Click Options > Shared Folders.
2. Under Folders you are sharing next to the user you want to remove access, click Delete.
3. Click Save.

Setting Up and Removing the Sent Folder

By default, copies of sent messages are not retained in your mailbox. Saved copies of sent messages occupy space in your mailbox and count against your mailbox quota. You can, however, designate a folder to store copies of sent messages.

NOTE: If you use both an IMAP mail client and WebAccess (for example, you use an IMAP mail client on your desktop computer, but you use WebAccess on your laptop), create a WebAccess folder matching your IMAP mail client's Sent folder. Then, select that folder as your Sent folder in WebAccess. Matching the Sent folder names in WebAccess and your IMAP mail client enables the folders to synchronize when you switch back and forth between mail systems. Some IMAP mail clients might work differently.

To designate a folder to collect sent messages:

1. Create a new folder to store sent messages. For more information, see "Adding Mailbox or Calendar Folders" on page 140.

   For example, create a folder named "Sent Messages."
2. Click Options > Mailbox Management.
3. Under Mailbox Settings, from the Sent Folder drop-down list, select the folder you created.
4. Click Save.

To disable the folder collecting sent messages:

1. Click Options > Mailbox Management.
2. Under Mailbox Settings, from the Sent Folder drop-down list, select Disable.
3. Click Save.

Deleting Folders

You can delete an entire folder and its contents.

IMPORTANT: Use care in deleting folders. When a folder is deleted, you cannot undelete it.

1. From the Folder List, click Delete Folder.
2. Select the Folder you want to delete.
3. Click OK.

Using Address Books

WebAccess address books store information about users and organizations that is displayed in HTML format. Using an address book, you can search for contact information to add e-mail addresses to a message, appointment, task, or note.

Within WebAccess, there are three types of address books:

- **Personal Address Book** stores information about your personal or professional contacts.
- **System-Wide Address Book** is typically a directory of names for your organization. Your administrator can give you rights to use system-wide address books.
- **Public Address Book** is typically a public LDAP server on the Internet (such as the Bigfoot directory service). Your administrator can give you rights to use public address books.

Before you can access a system-wide or public address book your administrator has made available, you need to configure a public LDAP Server. For more information, see "Configuring a Public LDAP Server" on page 186.

When you are sending, forwarding, or replying to a message, appointment, task, or note, you can use the address book to address recipients.

This section covers the following tasks:

- "Adding Contacts to Items from Address Books" on page 143
- "Searching for Contacts in Address Books" on page 143
- "Adding Contacts to a Personal Address Book" on page 144
- "Creating Personal Groups" on page 145
- "Setting Privacy Settings" on page 145
- "Configuring a Public LDAP Server" on page 145

Adding Contacts to Items from Address Books

You can use the three types of available address books to add contacts to mail messages, appointments, tasks, and notes.

1. Click Address Book  .
2. Click Create to add an entry.
3. Type the contact's name as you want it to appear in the Address Book.
4. If you want to send messages to the entry, type an e-mail address in the E-Mail Address field.
5. Add information to the other fields as desired.
6. Any information you add is displayed when you select the entry in the Address Book.
7. Click OK.

Searching for Contacts in Address Books

You can search for contacts from the three types of available address books, including:

- Personal Address Book
- System-wide Address Book
- Public Address Book

To search for contacts in one of the three types of address books:

1. Click Address Book  .

   or

When composing an item, click Address Book after clicking within the To, CC, BCC, Required, Optional, or Not Attending fields.

2. Under the Search For field, click the check box by the address book you want to include in the search.
3. Type a first or last name in the Search For field to find a specific contact.

   Single-letter search criteria function as wildcards. For example, if you type "J" as the search condition, the search returns all entries beginning with "J."

   The Search For field is not case sensitive. For example, Earl Nelson is the same as earl nelson.

   or

   Leave the Search For field empty to list all addresses from the personal address book. (Ensure Personal is selected.)
4. Click Search.

   When you click Search, a display of entries appears, matching your search criteria.
5. Click OK.
6. When the recipient's name appears, click the check box next to the name, click the recipient type (To, CC, or BC), and click Compose to continue to create your message, appointment, task, or note.

   For more information, see "Sending Mail Messages" on page 116, "Scheduling Appointments" on page 122, "Assigning Tasks" on page 128, and "Writing Notes" on page 133.

Adding Contacts to a Personal Address Book

You can add contacts to your personal address book in two ways. You can go directly to the address book and add the contact information or you can open a received message to add a new contact.

To add contacts to a personal address book:

1. Click Address Book  .
2. Under Personal, select Create.
3. Fill in the First Name and Last Name fields.
4. Type an e-mail address if you want to send messages to the contact.
5. Type information in the other fields as desired.
6. Click OK.

To add contacts to a personal address book from a received item:

1. From the INBOX item list or other folder, locate the received item from the contact you want to add to your personal address book.
2. Click the contact name in the From line of the message.

   For example, Steve Johnston

   A window appears allowing you to add a new personal address book entry.
3. Type in any additional information you want to add to any blank fields.
4. Click OK.

Creating Personal Groups

A group is a list of users you can send messages to by selecting the group name rather than selecting or typing each individual name or address. When you select a personal group as the recipient for a message, appointment, task, or note, all the individuals in the group receive the item. For example, a manager could create a personal group for all direct reports. The manager could then use the personal group to schedule team meetings, send a task for project status reports, or communicate general information to the team.

You can create and store personal groups in your Personal Address Book. Only you have access to your personal groups.

To create a personal group:

1. Click Address Book  .
2. Click Create.
3. In the First Name or Last Name field, enter a name for your personal group.
4. In the E-Mail Address field, enter the e-mail addresses of each individual you wish to include in your personal group. Each address entry can be delimited by either a semi-colon, a comma, or a space.
5. Click OK.

The personal group now appears in your Personal Address Book. When you select a personal group as the recipient for a message, all the individuals in the group will receive the message.

Setting Privacy Settings

You can choose how much system-wide address book information you want to share with other WebAccess users. You can hide or share the first name, last name, e-mail address, or phone number.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Privacy feature.

To set privacy settings:

1. Click Options  > General Settings.
2. Under Address Book Settings, use the Privacy drop-down list to select a privacy level, including the following levels:
   - **None**. All WebAccess users are given access to your first and last name, e-mail address, and phone number if this information is available.
   - **Limited**. All WebAccess users are given access only to your name and e-mail address.
   - **Unlisted**. No WebAccess users are given access to your personal information.
3. Click Save.

Configuring a Public LDAP Server

If you want to access public address books, you need to configure a public LDAP Server for your personal use. Public address books are derived from LDAP servers on the Internet (such as the Bigfoot directory service).

NOTE: Depending on how your administrator has configured your system, you might not have access to the Public LDAP Server feature.

To configure a public LDAP server:

1. Click Options  > General Settings.
2. Under Address Book Settings, provide the host name or IP address of the public directory you want to use in the Public LDAP Server field.
3. Click Save.

Using Rules

Use rules to define actions that you want automatically performed on the messages, appointments, tasks, or notes you receive or send. Rules can help you organize your mailbox, automate your mailbox while you are away, delete unwanted items, and save you time.

Rule actions include:

- **Move To:** Moves an item to the folder you specify. For example, you receive a monthly e-mail newsletter. When the newsletter arrives, you can have a rule move it to a folder to read later.
- **Delete:** Marks an item you specify as deleted. For example, if your ISP limits e-mails up to 10 KB and your system crashes when you receive a larger e-mail, you can set up a rule to delete incoming e-mails larger than the specified amount.
- **Forward To:** Forwards an item to the recipients you specify. For example, when you are away on vacation, you can have a rule automatically forward specified mail to a co-worker.
- **CC To:** Adds a designated address to the CC field. For example, when you receive e-mails about new job openings, you can have a rule automatically forward messages to a personal group of contacts looking for jobs.
- **Accept:** Accepts new appointments, tasks, or notes that your specify. For example, when you receive an appointment from your supervisor, you can have a rule automatically accept the appointment and add it to your calendar.
- **Decline**: Declines new appointments, tasks, or notes that your specify. For example, if repeatedly receive an appointment a sales person wanting to meet with you, you can have a rule automatically decline the appointment.
- **Stop Processing**: Stops processing the conditions of rule or any additional rules. NetMail executes conditions within a rule and the rules until a condition is found true. When the condition or rule is found true, it will stop processing any additional conditions or rules.

You can apply the rule to all new items or only new items that meet your established criteria.

When setting up rules, you define any specified conditions. For example, you might want to move all items you receive from your supervisor to a specific folder. You can define a condition so that only messages with your supervisor's name on the From line are moved to that folder. All other items remain in your INBOX item list.

When setting up the rules, you can move the conditions up or down on the list.The conditions within a rule are executed in preceding order first to last and the rules are executed in preceding order first to last.

This section covers the following tasks:

- “Creating Rules” on page 147
- “Activating and Deactivating Rules” on page 149

- “Deleting Rules” on page 149

Creating Rules

When you create a new rule, you need to do the following:

- Determine whether you want to set up a simple or advanced rule.
  - **Simple Rules** allow you to set up rules so all or any of the conditions are met before proceeding with any actions.
  - **Advanced Rules** allow you to set up rules that include and/or conditions. These are in preceding order from top to bottom.
- Define the condition or conditions for the rule.

  For example, you can have the rule search for your supervisor’s e-mail address.
- Define the action or actions you want the rule to run when the conditions are met.

  For example, when an incoming message comes into your mailbox and includes your supervisor’s e-mail address, you can set up a rule to forward your supervisor’s e-mails into a specified folder.

To create a rule:

1. Click Options  > Rules > Create New Rule.
2. Select Simple > Any or All as appropriate to your rule.

   If only one condition statement is needed, you can use either All or Any.

   or

   Select Advanced.
3. Define the rule condition.

   3a In the first drop-down list, define which Message Field option you want to monitor, such as From, To, Subject, and so forth.

   For example, if you want to move all messages from a specific sender to a separate folder, select From as the Message field options you want to monitor.

   3b In the second drop-down list, define the condition for the rule.

   For example, when you select From, the second drop-down list allows you to select either Contains or Does Not Contain. If you select Contain, all messages that contain your sender’s e-mail address are monitored as part of the condition of the rule.

   The condition options vary depending upon the Message Field option you select. For example, if you change the Message Field option to Size, the Condition options are More Than or Less Than.

   3c In the Variable Information field, specify the condition criteria.

   For example, in our previous scenario, you would type the sender’s e-mail address.

   The following information shows you available Condition options for your Condition Statement:

Condition drop-down list (Message Field Options)	Condition drop-down list (Secondary Condition Options)	Variable Information
From	contains or does not contain	text

To	contains or does not contain	text
Subject	contains or does not contain	text
CC	contains or does not contain	text
Header	contains or does not contain	text (in field)/ text
Body	contains or does not contain	text
Size	is more than or is less than	size in KB
Calendar Item	does not conflict or conflicts	NA
Attachment	MIME type Is or MIME type is not	MIME type
Apply to All Messages	NA	NA

4 Click plus (+) or minus (-) to add and remove up to 15 condition statements.

5 Use the OR/AND operators to define how each condition statement is applied (for Advanced rules only).

6 Define the rule action.

6a In the first drop-down list, define the action that you want performed, such as Move To, Delete, Forward To, and so forth.

For example, if you want to move all messages you receive from a specific sender to another folder, select Move To.

6b In the second drop-down list, define the completion of the action.

For example, if you want select Move To, the drop-down list allows you to select which folder you want to move the messages to.

The following table shows the available action options:

First Action drop-down list	Second Action drop-down list/Field/NA
Move To	drop-down list of available folders, such as INBOX, Sent, etc.
Delete	NA
Forward To	e-mail address
CC To	e-mail address
Accept	NA
Decline	NA
Stop Processing	NA

7 Click plus (+) or minus (-) to add and remove up to 15 Action statements.

8 If applicable for your rule, add any additional information required.

For example, you might need to provide the e-mail address of your supervisor to save the messages into a different folder.

9 Use the Perform The Following Action drop-down list or menus (as appropriate to your rule) to complete the If Statement for your rule.

For example, if you are setting up a Move To rule and you want to move all messages that meet your condition to a folder you created called “Urgent,” select the Urgent folder from the Move To drop-down list.

10 Click Save.

Activating and Deactivating Rules

Instead of deleting a rule that you do not want to run, you can deactivate a rule, allowing you to reactivate it for use in the future. When needed, you can reactivate the rule. If you want to delete a rule, see “Deleting Rules” on page 149.

To activate a rule:

1 Click Options > Rules.

2 Under Active on the rule you want to activate, click No to activate it.

This option is a toggle. When you select No, it changes it to Yes.

3 Click Save.

To deactivate a rule:

1 Click Options > Rules.

2 Under Active on the rule you want to deactivate, click Yes to deactivate it.

This option is a toggle. When you select Yes, it changes it to No.

3 Click Save.

Deleting Rules

You can delete the rules you create or you can deactivate rules. For more information, see “Activating and Deactivating Rules” on page 149.

IMPORTANT: Use care in deleting rules. When a rule is deleted, you cannot retrieve it.

1 Select Options > Rules.

2 Under Active, select Delete next to the rule you want to delete.

Downloading Messages from Other Accounts

If multiple e-mail accounts exist, you can set up WebAccess to routinely retrieve messages from your other accounts.You can also choose to leave copies of your incoming mail on the server, allowing you to access your mail from all your accounts.

This section covers the following tasks:

- “Downloading Mail Messages from Other Accounts” on page 149
- “Enabling and Disabling the Leave on Server Option” on page 150

Downloading Mail Messages from Other Accounts

Mail Proxy is a feature that allows you to retrieve messages sent to other e-mail accounts. For example, if you have e-mail accounts at work, home, and school, you can configure WebAccess to copy or move any new messages from those accounts to your mailbox.

Before configuring your proxy settings, you need to understand the following:

- The e-mail accounts must run on a POP3 or IMAP service. You cannot retrieve mail from Web only services such as Hotmail* or Yahoo*.
- Message retrieval is not instantaneous. The Proxy service runs at intervals set by your system administrator (every 1, 2, or 3 hours). Updates to your account occur on this preset schedule.
- You can proxy up to three e-mail accounts.
- Some e-mail providers allow access to your mailbox only if you log in within a specified IP address range that belongs to the service. These providers assign you an IP address upon login. In these cases, Proxy does not work even if it is a POP3 or IMAP e-mail service.
- You need to know the Host Name of the POP or IMAP server for your service provider, such as imap.myisp.com, mail.myisp.com, or pop.mail.myisp.com. If you do not know the host name, contact your service provider.

NOTE: Depending on how your administrator has configured your system, you might not have access to download messages from other accounts.

To download messages from other accounts:

1. Click Options  > Proxy Settings.
2. In the Host Name field, type the host name of the POP or IMAP server of your service provider.

   For example, the host name format is imap.myisp.com, mail.myisp.com, or pop.mail.myisp.com. If you do not know the host name, contact your service provider.
3. In the User Name field, type your user name for that account.

   For example, lmarshal.
4. In the Password field, type your password for that account.

   For example, password123.
5. Use the Type drop-down list to select IMAP or POP3.

   For the Proxy feature to work, POP3 and IMAP service is required for foreign mail accounts.

   Also, you cannot retrieve mail from Web-only mail services such as Yahoo or HotMail.
6. If you want to leave copies of your mail in your original mailbox, click the check box.

   For more information, see "Enabling and Disabling the Leave on Server Option" on page 150.
7. Click Save.

Enabling and Disabling the Leave on Server Option

You might want to leave the mail on the server if you are accessing your mail from client other than WebAccess.

When you leave mail on a server, it takes up server space. Because you are usually allotted a limited amount of space, we recommend that you leave it unselected unless sufficient space exist.

To enable the Leave on Server option:

1. Select the Leave on Server check box.

To disable the Leave on Server option:

1. Deselect the Leave on Server check box.

Giving Users Proxy Access to Your Mailbox and Calendar

Administrative assistants, co-workers, and others might need to access your mailbox to manage and process your incoming mail messages, appointments, tasks, or notes.

Two levels of rights exist:

- **Read Only** Allows those granted access to view your personal mailbox and calendars.
- **Read, Compose, and Delete.** Allows those granted access to view, edit/add, and remove items contained in your personal mailbox or calendars.

NOTE: You can hide some folders and calendars in your mailbox from proxy users. For more information, see "Hiding Folders" on page 140.

To give proxy rights to other users to your mailbox and calendar:

1. Click User Proxy  .
2. Under Grant proxy rights to another user, type the user name of the person you want to give proxy rights.

   The person is automatically granted Read Only rights.
3. If desired, click the Allow full rights option to give the person Read, Compose, and Delete rights.
4. Click Save.

To restrict access to previously granted rights:

1. Click User Proxy  .
2. Under Users who are allowed to act as proxy for you, click the Restrict Access option.

   The person rights are restricted to Read Only rights.

To delete user from proxy access:

1. Click User Proxy  .
2. Under Users who are allowed to act as proxy for you, click Delete  .

   The person is deleted from accessing your mailbox and calendar.

Changing Password and Secret Question/Answer Information

(October 7, 2003) Not available in WebAccess. Is this the intent? (September 18, 2003) Greg, no, it should be there.

Within WebAccess, you can change your password and question/answer at any time.

When you first set up an account with WebAccess, you are assigned a password or you provided a password, depending upon how your WebAccess is administered. You can change your password at any time. Passwords are case sensitive.

When you first set up an account with WebAccess, you are asked for a secret question and answer to help remind you of your user information. You can also change your question and answer.

To change your password:

1. Click Options  > General Settings.

2 Under Change Your Password, type your existing password in the Type Your Old Password field.

3 Type your new password in the Type Your New Password and Retype Password fields.

4 Click Save.

To change your secret question and answer:

1 Click Options > General Settings.

2 Under Change Your Secret Question and Answer, type your new question in the New Question field.

3 Type your new answer in the New Answer field.

4 Click Save.

Changing WebAccess Settings

This section covers the following tasks:

- "Changing the Timeout Setting" on page 152
- "Changing Language and Encoding Settings" on page 152
- "Changing from WebAccess to Webmail" on page 153
- "Changing Number of Messages Listed Per Page" on page 153

Changing the Timeout Setting

Specific actions, such as opening and item, sending an item, or composing a message without sending it, generate a call to the Web server. Other actions, such as scrolling through items in the item list, or reading Help topics, do not generate a call to the Web server. If, for a period of time, you leave WebAccess alone or perform actions that do not generate a call, WebAccess logs you out. Doing so not only provides security for your e-mail, but also ensures that the Web server and WebAccess run efficiently. When you are logged out, if you attempt to perform an action, you are prompted to log in again.

NOTE: Depending on how your administrator has configured your system, you might not have access modify the timeout setting.

To change the timeout setting:

1 Click Options > General Settings.

2 Under WebAccess Settings, type a timeout interval (from 1 to 40 minutes) in the Timeout field.

3 Click Save.

Changing Language and Encoding Settings

If you are experiencing problems with correct character display in WebAccess, verify that the language and character-set encoding are configured properly.

To enable WebAccess to display information in the language of your choice, you need to:

- Set the language to ensure that your WebAccess language setting matches the language in which you normally receive messages.
- Select the encoding that supports the selected language.

When WebAccess receives encoded information, it uses the currently selected character-set definition to display the information. It also uses the character-set definition to encode all outgoing messages. For this reason, you need to ensure that correct character-set encoding is selected for your language.

To change language settings:

1. Click Options > General Settings.
2. Under WebAccess Settings, use the Language drop-down list to select your language.
3. Click Save.

   Language changes are immediately implemented.

To change encoding settings:

1. Click Options > General Settings.
2. Under WebAccess Settings, use the Default Charset drop-down list to select the appropriate character-set encoding for your language.

   IMPORTANT: On Windows workstations, WebAccess uses Windows encoding to display characters. On other platforms, WebAccess uses ISO encoding. If both encoding types are displayed, choose the encoding that is appropriate for your platform.
3. Click Save.
4. Exit WebAccess and log back in for the changes to take effect.

Changing from WebAccess to Webmail

NetMail offers two Web interfaces, WebAccess and Webmail.If your administrator has enabled it, you can use either interface.

To change template settings:

1. Click Options > General Settings.
2. Under WebAccess Settings, use the Select Template drop-down list to select Webmail.
3. Click Save.
4. To activate the new template, exit WebAccess, and then log back in again.

Changing Number of Messages Listed Per Page

You can determine the number of messages appearing per Web page inside your various folders. The default number of messages per page is 10. You can choose to display from 5 to 50 messages per page. When messages are spread over multiple pages, click Next to view each successive page.

To change number of messages per page:

1. Click Options > General Settings.
2. Under WebAccess Settings, use the Messages Per Page drop-down list to select the number of messages you want to display per page.
3. Click Save.

Changing Time and Date Settings

This section covers the following tasks:

- "Setting the Time Zone Setting" on page 154
- "Setting the Short or Long Date Format" on page 154
- "Setting the Time Format" on page 154
- "Setting the First Day of the Week" on page 155

Setting the Time Zone Setting

To ensure that dates and times are correct in messages, appointments, and other time-relevant information, you must indicate to WebAccess the time zone for your location. The time is then automatically adjusted for appointments sent between people in different time zones.

For example, if you are located in New York and schedule a conference call with people in Los Angeles for 4:00 p.m. your time, the appointment received by the Los Angeles recipients shows the conference call at 1:00 p.m. their time.

For your message to appear with the correct time stamp, you must ensure that your time zone is set correctly.

To change your time zone setting:

1. Click Options  > General Settings.
2. Under Time and Date Settings, use the Time Zone drop-down list to select the appropriate time zone.
3. Click Save.

Setting the Short or Long Date Format

You can change the date format within WebAccess.

To change the short date format:

1. Click Options  > General Settings.
2. Under Time and Date Settings, use the Short Date Format drop-down list to select the format of your choice.
3. Click Save.

To change the long date format:

1. Click Options  > General Settings.
2. Under Time and Date Settings, use the Long Date Format drop-down list to select the format of your choice.
3. Click Save.

Setting the Time Format

You can change the time format within WebAccess.

1. Click Options  > General Settings.
2. Under Time and Date Settings, use the Time Format drop-down list to select the format of your choice.
3. Click Save.

Setting the First Day of the Week

1. Click Options  > General Settings.
2. Under Time and Date Settings, use the First Day of the Week drop-down list to select the first day of the week.
3. Click Save.

Using Webmail

Webmail is an easy-to-use, Web-based messaging system that offers a wide range of powerful communication and collaboration capabilities. It requires no JavaScript support and runs within any browser that is compatible with HTML 2.0+ and above.

Webmail enables you send and receive messages, appointments, tasks, notes, and attached files. Additionally, you can keep track of your schedule with the calendar, search for times when participants and resources (such as conference rooms) are available for a appointments, and manage folders.

Webmail is for use with lower-end browsers. If your browser is a higher-end browser, use the WebAccess interface instead. To change to the WebAccess interface, see "Changing from Webmail to WebAccess" on page 192.

This section covers the following tasks:

- "Starting and Exiting the Webmail Interface" on page 155
- "Viewing and Sending Mail Messages" on page 156
- "Forwarding Items" on page 160
- "Replying to Items" on page 161
- "Scheduling Appointments and Using the Calendar" on page 162
- "Using Tasks" on page 168
- "Using Notes" on page 173
- "Managing Mail Messages" on page 177
- "Managing Folders" on page 180
- "Using Address Books" on page 183
- "Using Rules" on page 187
- "Downloading Mail from Other Accounts" on page 189
- "Giving Users Proxy Access to Your Mailbox and Calendar" on page 190
- "Changing Webmail Settings" on page 191
- "Changing Time and Date Settings" on page 193

Starting and Exiting the Webmail Interface

If you set Webmail as your default client when you set up your NetMail account, Webmail opens when you type the NetMail URL and log in. If the WebAccess interface opens and you want to change to the Webmail interface, see "Changing from WebAccess to Webmail" on page 153.

You start Webmail by providing an URL that you obtain from your administrator. You need a username and password to log in.

To start and log in to Webmail:

1. Specify the URL for NetMail obtained from your administrator.
2. Specify your user name.

   The username (or User ID) is not case sensitive. For example, MargaretV is the same as margaretv.
3. Specify your password.

   The password is case sensitive. For example, AAGGHJKL is not the same as aagghjkl.
4. Click OK.

To exit and log out of Webmail:

1. Click Logout.

   Use Logout to properly log out, rather than just closing your browser.

.

Viewing and Sending Mail Messages

The main function of the Webmail mail system is to view and send e-mail messages.

This section covers the following tasks:

- "Viewing Received and Sent Mail Messages" on page 156
- "Viewing and Saving Attachments" on page 157
- "Sending Mail Messages" on page 157
- "Sending Mail Messages with Attachments" on page 158
- "Adding and Removing a Signature on Outgoing Items" on page 159

Viewing Received and Sent Mail Messages

Received messages are messages that arrive your mailbox. Sent messages are the messages that you send to other recipients. You can view both received and sent messages.

IMPORTANT: By default, copies of sent messages are not retained in your mailbox. Therefore, you must set up a folder for sent messages before you can view sent messages. For more information, see "Setting Up and Removing the Sent Folder" on page 182.

To view a received message:

1. Click Folders > INBOX.
2. Click the message you want to open.

   The mail message appears, allowing you to view, forward, reply to, delete, and view the source.

   (Oct. 7, 2003 - not completely updated). You can also Accept, Decline, Delegate, and Complete a mail message from this dialog. This is not the correct functionality for a mail message. Functions not available, but available in WebAccess include: Change Message Options (priority, public/private, changing message as unread), or print. Greg note (Sept 15,

2003): The functions not available should be here. Also, Quick Delete is changing to Purge All.

To view a sent message:

1. Click Folders.
2. Click the folder you created for sent messages.
3. Click the sent message you want to view.

Viewing and Saving Attachments

All Webmail items you send or receive can include attachments of any file type (for example, text, audio, image, video, and application).

When you view an unidentified attached file, Webmail attempts to convert the file to HTML and opens it in your browser. If Webmail cannot convert the file, try opening the file within your browser. Depending on how your browser is configured, you can expect the browser to do one of the following: display the file, launch an application to view the file in its native format, or save the file.

When NetMail sends a message, it encodes attachments in base64, which increases the size of the attachment 25 to 30 percent from the original file.

To view an attachment:

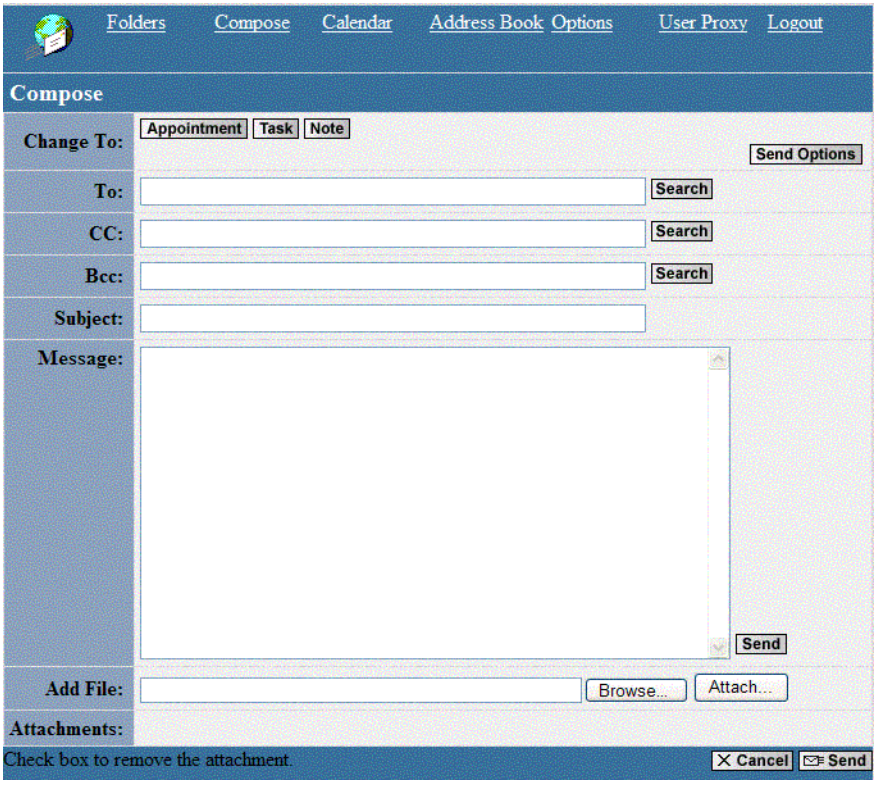
1. Locate and click the mail message that contains the attachment you want to view.
2. Click attachment.
3. Click Open.

To save an attachment in its native format:

1. Locate and click the mail message that contains the attachment you want to view.
2. Click attachment.
3. Click Save, then click Close.

Sending Mail Messages

Description: Compose Mail Message window in Webmail



To send a message:

1. Click Compose.
2. In the To, CC, or BC fields, add recipients' e-mail addresses, separated by a semicolon, a comma, or a space.

   or

   In the To, CC, or BC fields, click Search to access the Address Book. For more information, see "Using Address Books" on page 183.
3. Type a subject and message in the subject and Message fields.
4. Click Send Options to set the message priority and the delivery status notification.

   For more information, see "Setting the Mail Message Priority" on page 177 and "Setting Delivery Status Notification" on page 178.
5. Click Send.

Sending Mail Messages with Attachments

All Webmail items you send or receive can include attachments of any file type (for example, text, audio, image, video, and application).

You can attach one or more files to an item to send to other users. For example, you might want to send a document in a mail message to another user.

When NetMail sends a message, it encodes attachments in base64, which increases the size of the attachment 25 to 30 percent from the original file.

To attach files to an item, your browser must support attachments.

To send a message with an attachment:

1. Click Compose.
2. In the To, CC, or BC fields, add recipients' e-mail addresses and, separated by a semicolon, a comma, or a space.

   or

   In the To, CC, or BC fields, click Search to access the Address Book. For more information, see "Using Address Books" on page 183.
3. Type a subject and message in the subject and Message fields.
4. For each file you want to attach, do the following:

   4a. Click Browse to locate the file you want to attach.

   4b. Click the file, then select Open.

   4c. Click Attach.

   To remove any attachments, click the Remove option next to each attachment before sending.
5. Click Send Options to set the message priority and the delivery status notification.

   For more information, see "Setting the Mail Message Priority" on page 177 and "Setting Delivery Status Notification" on page 178.
6. Click Send.

Adding and Removing a Signature on Outgoing Items

A signature provides contact information that is automatically included at the end of messages, appointments, tasks, and notes that you send.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Signature feature.

To add a signature on outgoing items:

1. Click Options > Mailbox Management.
2. Under Signature, select Yes to the Enabled option.
3. In the Signature field, provide the information you want to appear at the bottom of each message you send.

   Sam Marshall
   My Company
   Office of IT
   smarshal@mycompany.com
   405-423-7323
4. Click Apply.

To remove a signature on outgoing items:

1. Click Options > Mailbox Management.
2. Under Signature, select No to the Enabled option.
3. Click Apply.

Forwarding Items

You can individually forward messages, appointments, tasks, and notes to a recipient or another e-mail account or you can set up automatic forwarding to forward all incoming messages to another recipient or e-mail account.

NOTE: You can use the Rules feature to forward incoming messages to specific folders, recipients, or e-mail accounts under defined conditions. For more information, see "Using Rules" on page 187.

This section covers the following tasks:

- "Forwarding Mail Messages, Appointments, Tasks, and Notes" on page 160
- "Setting Up and Removing Automatic Forwarding" on page 160

Forwarding Mail Messages, Appointments, Tasks, and Notes

1. Locate and click the message you want to forward to open it.
2. Click Forward.
3. In the To, CC, or BC fields, add recipients' e-mail addresses, separated by a semicolon, a comma, or a space.

   or

   In the To, CC, or BC fields, click Search to access the Address Book. For more information, see "Using Address Books" on page 183.
4. Type an additional message in the Message field.
5. Click Send.

Setting Up and Removing Automatic Forwarding

You can use the Automatic Forwarding feature to automatically forward all incoming messages to a recipient or e-mail account.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Automatic Forwarding feature.

To set up automatic forwarding:

1. Click Options > Mailbox Management.
2. Under Forwarding, select Yes for the Enabled option.
3. If you want to keep copies of your messages in your mailbox, select Yes for the Keep Copy option.

   IMPORTANT: If you select No for this option, forwarded messages no longer exist in the Webmail account.
4. Type one or more e-mail addresses in the Forward To field.

   Use Return to move to the next line and list one e-mail address per line.
5. Click Apply.

To remove automatic forwarding

1. Click Options > Mailbox Management.
2. Under Forwarding, select No for the Enabled option.
3. Click Apply.

Replying to Items

When you receive items, you can send a reply message directly to the original sender of the message or you can reply to all the recipients included on the original message.

You can also set up and remove an automatic reply to the sender or original recipients.

NOTE: You can use the Rules feature to automatically respond to specific messages under defined conditions. For more information, see "Using Rules" on page 187.

This section covers the following tasks:

- "Replying to Received Mail Messages, Appointments, Tasks, and Notes" on page 161
- "Setting Up and Removing an Automatic Reply" on page 161
- "Providing a Different Address for a Reply" on page 162

Replying to Received Mail Messages, Appointments, Tasks, and Notes

In addition to accepting or declining an appointment, task, or note, you can also send a reply message to the original sender of the message or to all recipients.

To reply to messages, appointments, tasks, and notes:

1. Locate and click the item you want to reply to either from the INBOX folder or calendar, depending upon whether the item is accepted.
2. Click Reply or Reply All.

   Reply sends your response to the original sender. Reply All sends your response to the original sender and everyone that was included as a recipient.
3. Type an additional message in the Message field.
4. Click Send.

Setting Up and Removing an Automatic Reply

When you are unavailable and you cannot retrieve your messages for an extended period of time (such as when you are away at a conference, vacation, or tied up in meetings), you can set up an automatic reply with a message. When you return, immediately remove your automatic reply.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Automatic Reply feature.

To set up an automatic reply:

1. Click Options > Mailbox Management.
2. Under Auto-reply/Vacation Message, select Yes for the Enabled option.
3. In the Message field, type the message you want to include in your automatic reply.

   For example:

   ```
   I am on vacation from April 1 to April 15. If you need anything during
   that time, please contact Brian Thompson at bthompson@mycompany.com.
   ```
4. Click Apply.

To remove an automatic reply:

1. Click Options > Mailbox Management.

2 Under Auto-reply/Vacation Message, select No for the Enabled option.

3 Click Apply.

Providing a Different Address for a Reply

If you do not want recipients to have your individual e-mail address for your current mailbox, you can specify a different e-mail address that the system automatically uses when recipients reply to your messages. The Reply To address appears on the From: line of all your outgoing mail.

For example, if you use your account for a customer survey, you might want the survey respondents to return their responses to another e-mail address so they cannot contact you directly in the future.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Reply To address feature.

To configure your Reply To address:

1 Click Options > General Settings.

2 Under General Settings, specify your preferred Reply To e-mail address in the Reply To field.

IMPORTANT: Specifying a different address for a reply does not automatically enable you to receive mail at that address. You must provide an existing Internet e-mail address, such as ruth@mywebmail.com.

3 Click Apply.

Now when you send a message and the recipient replies, the reply message is automatically addressed to the specified Reply To address.

To remove your Reply To address:

1 Click Options > General Settings.

2 Under General Settings, remove your preferred Reply To e-mail address in the Reply To field.

3 Click Apply.

Scheduling Appointments and Using the Calendar

The calendar lets you view appointments, tasks, or notes you receive from others or create to send to yourself. Using the calendar, you can view your schedule one day, one week, or one month at a time.

When accepted, the calendar displays all appointments, tasks, and notes you receive.

This section covers the following tasks:

- "Changing the Time Span of the Calendar View" on page 163
- "Scheduling Appointments" on page 163
- "Using Busy Search for People and Resources" on page 165
- "Accepting, Declining, and Delegating Appointments" on page 165
- "Using Multiple Calendars" on page 166
- "Marking Appointments Read or Unread (Read Later)" on page 167
- "Moving and Copying Appointments to Folders and Other Calendars" on page 167
- "Deleting and Undeleting Appointments" on page 168

NOTE: Depending on how your administrator has configured your system, you might not have access to the calendaring features.

Changing the Time Span of the Calendar View

Using the calendar, you can view your schedule one day, one week, or one month at a time. You can also change the year that you want to view.

To change the day:

1. Click Calendar.
2. Click Day.
3. From the Day drop-down list, click the day you want to view, then click Change To.

   or

   Click Today to change the calendar view to the current day.

To change the week:

1. Click Calendar.
2. Click Week.
3. From the Day drop-down list, click the day in the week you want to view, then click Change To.

   or

   Click Today to change the calendar view to the current week.

To change the month:

1. Click Calendar > Month.
2. From the Month drop-down list, click the month you want to view.

To change the year:

1. Click Calendar.
2. From the Year drop-down list, click the year you want to view, then click Change To.

Scheduling Appointments

Using the appointment feature, you can schedule appointments, people, or resources.

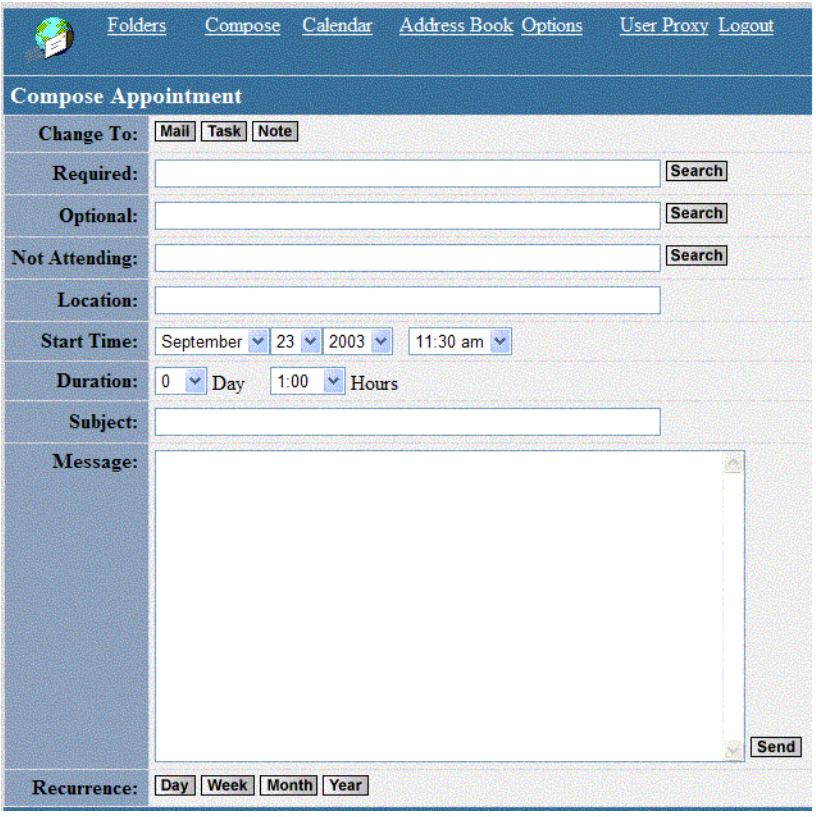
(October 7, 2003) The Busy Search feature is not yet available on the Webmail interface as expected.

The Busy Search Feature allows you to check people's schedules and resource availability to determine the best time to schedule an appointment. For more information on the Busy Search features, see "Using Busy Search for People and Resources" on page 165.

When you set up appointments, you can address recipients in Required, Optional, and Not Attending fields to indicate to recipients your intent and expectations in inviting them to the appointment. Recipients can then accept, decline, or delegate the appointment.

Use the Required field to schedule resources.

Description: Compose Appointment window in Webmail



To schedule an appointment:

1. Click Compose > Appointment.
2. In the Required, Optional, or Not Attending fields, type recipients' and resources' e-mail addresses, separated by a semicolon, a comma, or a space.

   or

   In the Required, Optional, or Not Attending fields, click Search to access the Address Book. For more information, see "Using Address Books" on page 183.

   or

   Leave all the recipient fields blank to create a personal appointment that appears only in your calendar.
3. Specify a location for the appointment.

   The Location field is only a text field, which allows you to provide a description of the location. However, to actually schedule a resource, you must specify the resource in the Required field.
4. Use the Start Time drop-down lists to specify a month, a day, year, and beginning time for the appointment.
5. Use the Duration drop-down lists to specify the number of days or hours.
6. Type a subject and message for the appointment in the Subject and Message fields.
7. If the appointment occurs on a regular basis, specify the recurrence settings. Select Day, Week, Month, and Year as appropriate.

The maximum value you can type for number of occurrences for recurring events daily, weekly, monthly, and yearly is 100.

7a Specify the appropriate number of days, weeks, months, or years before you want the appointment to reappear in the recipients' mailboxes.

7b Select one of the following options:

- No End Date.
- End after *x* occurrences, where *x* indicates the number of occurrences.
- End by Month, Day, Year, and Time. Use the drop-down lists to specify each one.

8 Click Send.

Using Busy Search for People and Resources

(Oct. 7, 2003 - Not yet available on the interface.) Is this expected for 3.5? (Greg review - "Should Be") Below are the anticipated steps. Need to test with interface if available this release.

You can use busy search to find out when people and resources (such as conference rooms) are available. It simplifies setting up appointments and saves times in scheduling with others.

To use busy search for scheduling people and resources:

1 Click Compose > Appointment.

2 In the Required, Optional, or Not Attending fields, type recipients' and resources' e-mail addresses, separated by a semicolon, a comma, or a space.

or

In the Required, Optional, or Not Attending fields, click Search to access the Address Book. For more information, see "Using Address Books" on page 183.

3 Specify a location for the appointment.

The Location field is only a text field, which allows you to provide a description of the location. However, to actually schedule a resource, you must specify the resource in the Required field.

4 Use the Start Time drop-down lists to specify a month, a day, year, and beginning time for the appointment.

5 Use the Duration drop-down lists to specify the number of days or hours.

6 Type a subject and message for the appointment in the Subject and Message fields.

7 Click Busy Search to find out what time participants and the conference room have free time or busy time.

If a critical participant is busy, click Cancel and reset the time. Then perform the busy search again if needed.

8 Click Send.

Accepting, Declining, and Delegating Appointments

When you receive an appointment invite, you can either accept it, decline it, or delegate it.

To accept an appointment:

1 Locate the appointment you want to accept from the INBOX folder.

2 Click the appointment to open it, then click Accept.

The appointment is deleted (not purged) from the INBOX folder and appears on your calendar.

To decline an appointment:

1 Locate the appointment you want to decline in either from the INBOX folder or calendar, depending upon whether the appointment is accepted.

2 Click the appointment to open it, then click Decline.

The appointment is deleted (not purged) from your mailbox.

To delegate an appointment:

1 Locate the appointment you want to delegate in either from the INBOX folder or calendar, depending upon whether the appointment is accepted.

2 Click the appointment to open it > Delegate.

3 Type the e-mail address of the person to whom you want to delegate the appointment, then add any comments in the Comment to Delegatee field.

4 Click Send.

The appointment is deleted (not purged) from your mailbox and sent to the delegatee you specified.

Using Multiple Calendars

Webmail gives you the benefits and capabilities of working with multiple calendars.

For example, you can maintain your own personal calendar, a general calendar for your organization, or calendars for various resources.

With multiple calendars, you can move or copy appointments, tasks, and notes between calendars.

NOTE: You can use the Rules feature to accept and move incoming appointments, notes, and tasks to a different calendar under defined conditions. For more information, see "Using Rules" on page 146.

To add multiple calendars to your account:

1 Click Folders > Create Folder.

2 In the Create Folder field, specify the name of your calendar.

3 Select Calendar as the type of folder you want to add.

By default, new folders are added at the root level of the mailbox.

4 Click Apply.

To move items between calendars:

1 Click Folders.

2 Click the calendar that contains the item you want to move.

3 Within the calendar, locate the item you want to move.

4 Click the check box to the left of the item you want to move.

5 Select the calendar where you want to move the item.

6 Click Apply.

To copy items between calendars:

1. Click Folders.
2. Click the calendar that contains the item you want to copy.
3. Within the calendar, locate the item you want to copy.
4. Click the check box to the left of the item you want to copy.
5. Select the calendar where you want to copy the item.
6. Click Apply.

Marking Appointments Read or Unread (Read Later)

You can mark an appointment to appear as if it is opened or unopened. For example, if you opened an appointment and are interrupted, you might want to mark the appointment as unread to remind you to read it later.

To mark an appointment read:

1. Locate the appointment you want to mark read in either the INBOX folder.
2. Click the check box to the left of the appointment you want to mark read.
3. Select Mark Read.

   The appointment is marked as read.

To mark an appointment unread:

1. Locate the appointment you want to mark unread in either the INBOX folder.
2. Click the check box to the left of the appointment you want to mark unread.
3. Select Mark Unread.

   The appointment is marked as unread.

Moving and Copying Appointments to Folders and Other Calendars

If the appointment is not accepted, you can move it to another folder. When you accept it, the appointment is deleted (not purged) from the INBOX folder and appears on your calendar. You can move or copy the accepted appointment from one calendar to another.

To move an appointment to another folder:

1. Locate the appointment you want to move from the INBOX folder.
2. Click the check box to the left of the appointment you want to move, then click Move.
3. Select the folder where you want to move the appointment.
4. Click Apply.

   The appointment is moved to the specified folder.

To copy an appointment to another folder:

1. Locate the appointment you want to copy from the INBOX folder.
2. Click the check box to the left of the appointment you want to copy, then click Copy.
3. Select the folder where you want to copy the appointment.
4. Click Apply.

The appointment is copied to the specified folder.

To move an accepted appointment to another calendar:

1. In your calendar, locate the appointment you want to move.
2. Click the check box to the left of the appointment you want to move, then click Move.
3. Select the calendar where you want to move the appointment.
4. Click Apply.

   The appointment is moved to the specified calendar.

To copy an accepted appointment to another calendar:

1. In your calendar, locate the appointment you want to copy.
2. Click the check box to the left of the appointment you want to copy, then click Copy.
3. Select the calendar where you want to copy the appointment.
4. Click Apply.

   The appointment is copied to the specified calendar.

Deleting and Undeleting Appointments

When appointments are deleted from the calendar, they are automatically purged.

IMPORTANT: Use care in deleting already accepted appointments, tasks, and notes. When these items are deleted, you cannot undelete them. The only time that you can undelete an appointment, task, or note, is if it still exists as a deleted item in the INBOX folder.

To delete an appointment:

1. Locate the appointment you want to delete from the INBOX folder.
2. Click the check box to the left of the appointment you want to delete, then click Delete.

   or

   Click the appointment to open it, then click Delete.

To undelete an appointment from the INBOX folder or another folder:

1. Locate the appointment you want to undelete from the INBOX folder or another folder.
2. Click the check box to the left of the appointment you want to undelete, then click Undelete.

Using Tasks

This section covers the following tasks:

- "Viewing Tasks" on page 169
- "Assigning Tasks" on page 169
- "Accepting, Declining, and Delegating Tasks" on page 170
- "Marking Tasks Completed" on page 171
- "Marking Tasks Read or Unread (Read Later)" on page 171
- "Moving and Copying Tasks to Folders and Other Calendars" on page 171
- "Deleting and Undeleting Tasks" on page 172

Viewing Tasks

You can view a task from the INBOX folder (before accepting or declining it) and from the calendar. Declined tasks are deleted (not purged) from your mailbox.

To view a received task:

1 From the INBOX folder or calendar, click the task you want to open.

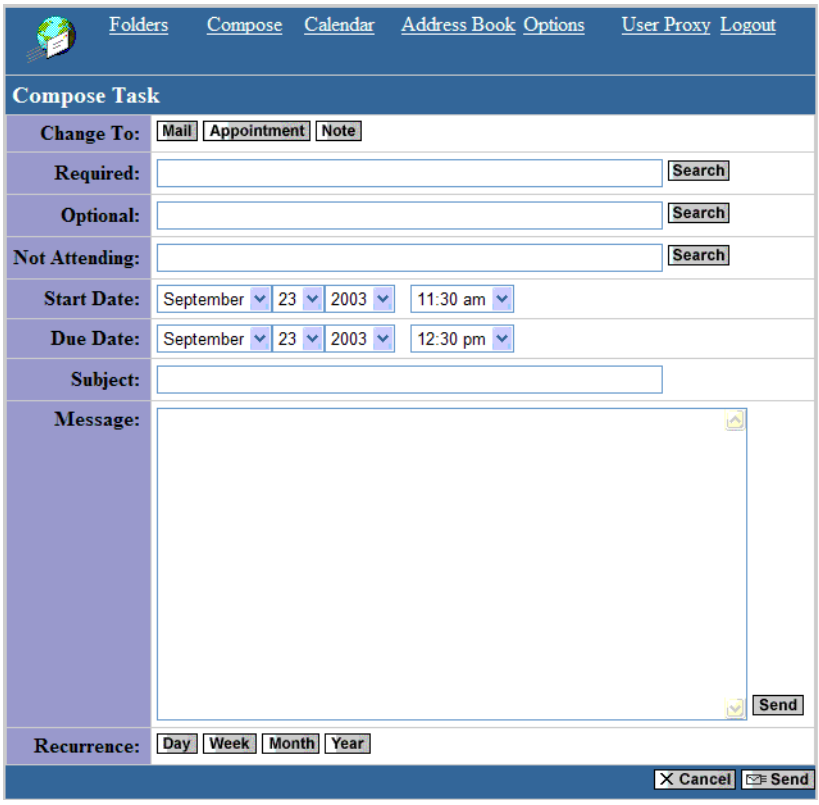
The task appears, allowing you to view, accept, decline, delegate, forward, reply to, delete, mark complete, and view the source.

Assigning Tasks

You can send tasks to yourself and others that appear on your personal calendar and other recipients' calendars. Recipients can choose to either accept or decline a task.

When you assign tasks, you can address recipients in Required, Optional, and Not Attending fields to indicate to recipients your intent and expectations in assigning the task.

Description: Compose Task window in Webmail



To assign a task:

1 Click Compose > Task.

2 In the Required, Optional, or Not Attending fields, type recipients' and resources' e-mail addresses, separated by a semicolon, a comma, or a space.

or

In the Required, Optional, or Not Attending fields, click Search to access the Address Book. For more information, see "Using Address Books" on page 183.

or

Leave all the recipient fields blank to create a personal task that appears only in your calendar.

3 Use the Start Date drop-down lists to specify a month, a day, year, and time that you want the task to appear on the recipient's calendar.

4 Use the Due Date drop-down lists to specify a month, a day, year, and time when you want the task completed.

5 Type a subject for the task in the Subject field.

6 Type the instructions or task description in the Message field.

7 Select Day, Week, Month, and Year as appropriate to set up a task recurrence.

7a Specify the appropriate number of days, weeks, months, or years before you want the task to reappear in the recipients' mailboxes.

7b Select one of the following options:

- No End Date.
- End after *x* occurrences, where *x* indicates the number of occurrences.
- End by Month, Day, Year, and Time. Use the drop-down lists to specify each one.

8 Click Send.

Accepting, Declining, and Delegating Tasks

When you receive a task, you can either accept it, decline it, or delegate it.

To accept a task:

1 Click Folders > INBOX.

2 Click the check box to the left of the task you want to accept, then click Accept.

or

Click the task to open it, then click Accept.

The task is deleted (not purged) from the INBOX folder and appears on your calendar.

To decline a task:

1 Click Folders > INBOX (if the task is not already accepted).

or

Click Calendar > the date of task you want to decline.

2 Click the check box to the left of the task you want to decline, then click Decline.

or

Click the task to open it, then click Decline.

The task is deleted (not purged) from your mailbox.

To delegate a task:

1 Click Folders > INBOX (if the task is not already accepted).

or

Click Calendar > the date of task you want to accept.

2. Click the task to open it, then click Delegate.
3. Type the e-mail address of the person to whom you want to delegate the task, then add any comments in the Comment to Delegatee field.
4. Click Send.

   The task is deleted (not purged) from your mailbox and sent to the delegatee you specified.

Marking Tasks Completed

When you complete a task, you can mark it completed to remove it from your mailbox.

1. From Calendar, select the date of the task you want to mark completed.
2. Click the check box to the left of the task you want to mark as complete, then click Complete.

   or

   Click the task to open, then select Complete.
3. Click Complete.

Marking Tasks Read or Unread (Read Later)

You can mark a task to appear as if it is opened or unopened. For example, if you opened a task and are interrupted, you might want to mark the task as unread to remind you to read it later.

To mark a task read:

1. Locate the task you want to mark read in either the INBOX folder.
2. Click the check box to the left of the task you want to mark read.
3. Select Mark Read.

   The task is marked as read.

To mark a task unread:

1. Locate the task you want to mark unread in either the INBOX folder.
2. Click the check box to the left of the task you want to mark unread.
3. Select Mark Unread.

   The task is marked as unread.

Moving and Copying Tasks to Folders and Other Calendars

If the task is not accepted, you can move it to another folder. When you accept it, the task is deleted (not purged) from the INBOX folder and appears on your calendar. You can move or copy the accepted task from one calendar to another.

To move a task to another folder:

1. Locate the task you want to move from the INBOX folder.
2. Click the check box to the left of the task you want to move, then click Move.
3. Select the folder where you want to move the task.

4. Click Apply.

   The task is moved to the specified folder.

To copy a task to another folder:

1. Locate the task you want to copy from the INBOX folder.
2. Click the check box to the left of the task you want to copy, then click Copy.
3. Select the folder where you want to copy the task.
4. Click Apply.

   The task is copied to the specified folder.

To move an accepted task to another calendar:

1. In your calendar, locate the task you want to move.
2. Click the check box to the left of the task you want to move, then click Move.
3. Select the calendar where you want to move the task.
4. Click Apply.

   The task is moved to the specified calendar.

To copy an accepted task to another calendar:

1. In your calendar, locate the task you want to copy.
2. Click the check box to the left of the task you want to copy, then click Copy.
3. Select the calendar where you want to copy the task.
4. Click Apply.

   The task is copied to the specified calendar.

Deleting and Undeleting Tasks

When tasks are deleted from the calendar, they are automatically purged.

IMPORTANT: Use care in deleting already accepted appointments, tasks, and notes. When these items are deleted, you cannot undelete them. The only time that you can undelete an appointment, task, or note, is if it still exists as a deleted item in the INBOX folder.

To delete a task:

1. Locate the task you want to delete from the INBOX folder.
2. Click the check box to the left of the task you want to delete, then click Delete.

   or

   Click the task to open it, then click Delete.

To undelete a task from the INBOX folder or another folder:

1. Locate the task you want to undelete from the INBOX folder or another folder.
2. Click the check box to the left of the task you want to undelete, then click Undelete.

Using Notes

Notes allow you to indicate the day you want the note to appear on the recipient's calendar. Because notes are posted in the recipient's calendar, you can use them as reminders of specific events, such as days off, project deadlines, or birthdays.

This section covers the following tasks:

- "Viewing Notes" on page 173
- "Writing Notes" on page 173
- "Accepting, Declining, and Delegating Notes" on page 175
- "Marking Notes Read or Unread (Read Later)" on page 175
- "Moving and Copying Notes to Folders and Other Calendars" on page 176
- "Deleting and Undeleting Notes" on page 176

Viewing Notes

You can view a note from the INBOX folder (before accepting or declining it) and from the calendar. Declined notes are deleted (not purged) from your mailbox.

1 From the INBOX folder or calendar, click the note you want to open.

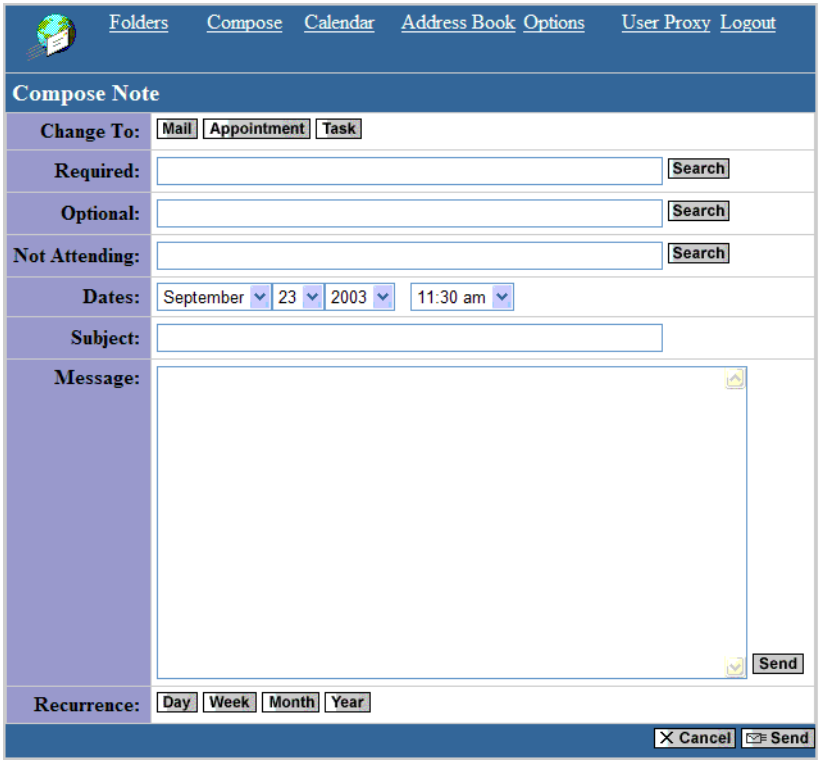
The note appears, allowing you to view, accept, decline, delegate, forward, reply to, delete, mark complete, and view the source.

Writing Notes

You can write notes that you want to appear on your personal calendar and other recipients' calendars. Because notes are posted in the recipient's calendar, you can use them as reminders of specific events, such as days off, project deadlines, or birthdays.

When you write notes, you can address recipients in Required, Optional, and Not Attending fields to indicate to recipients your intent and expectations in writing the note.

Description: Compose Note window in Webmail



To write a note:

1. Click Compose > Note.
2. In the Required, Optional, or Not Attending fields, type recipients' and resources' e-mail addresses, separated by a semicolon, a comma, or a space.

   or

   In the Required, Optional, or Not Attending fields, click Search to access the Address Book. For more information, see "Using Address Books" on page 183.

   or

   Leave all the recipient fields blank to create a personal note that appears only in your calendar.
3. Use the Date drop-down list to specify a month, a day, year, and time for the note to appear on recipients' calendars.
4. Type a subject and message for the note in the Subject and Message fields.
5. If you want the note to occur on a regular basis, specify the recurrence settings. Select Day, Week, Month, and Year as appropriate.

   5a Specify the appropriate number of days, weeks, months, or years before you want the note to reappear in recipients' calendars.

   5b Select an option.

   - No End Date.
   - End after *x* occurrences, where *x* indicates the number of occurrences.
   - End by Month, Day, Year, and Time. Use the drop-down lists to specify each one.
6. Click Send.

Accepting, Declining, and Delegating Notes

When you receive a note, you can either accept it, decline it, or delegate it.

To accept a note:

1. Click Folders > INBOX.
2. Click the check box to the left of the note you want to accept, then click Accept.

   or

   Click the note to open it, then click Accept.

   The note is deleted (not purged) from the INBOX folder and appears on your calendar.

To decline a note.

1. Click Folders > INBOX (if the note is not already accepted).

   or

   Click Calendar > the date of note you want to decline.
2. Click the check box to the left of the note you want to decline, then click Decline.

   or

   Click the note to open it, then click Decline.

   The note is deleted (not purged) from your mailbox.

To delegate a note:

1. Click Folders > INBOX (if the note is not already accepted).

   or

   Click Calendar > the date of note you want to accept.
2. Click the note to open it, then click Delegate.
3. Type the e-mail address of the person to whom you want to delegate the note, then add any comments in the Comment to Delegatee field.
4. Click Send.

   The note is deleted (not purged) from your mailbox and sent to the delegatee you specified.

Marking Notes Read or Unread (Read Later)

You can mark a note to appear as if it is opened or unopened. For example, if you opened a note and are interrupted, you might want to mark the note as unread to remind you to read it later.

To mark a note read:

1. Locate the note you want to mark read in either the INBOX folder.
2. Click the check box to the left of the note you want to mark read.
3. Select Mark Read.

   The note is marked as read.

To mark a note unread:

1. Locate the note you want to mark unread in either the INBOX folder.

2. Click the check box to the left of the note you want to mark unread.
3. Select Mark Unread.

   The note is marked as unread.

Moving and Copying Notes to Folders and Other Calendars

If the note is not accepted, you can move it to another folder. When you accept it, the note is deleted (not purged) from the INBOX folder and appears on your calendar. You can move or copy the accepted note from one calendar to another.

To move a note to another folder:

1. Locate the note you want to move from the INBOX folder.
2. Click the check box to the left of the note you want to move, then click Move.
3. Select the folder where you want to move the note.
4. Click Apply.

   The note is moved to the specified folder.

To copy a note to another folder:

1. Locate the note you want to copy from the INBOX folder.
2. Click the check box to the left of the note you want to copy, then click Copy.
3. Select the folder where you want to copy the note.
4. Click Apply.

   The note is copied to the specified folder.

To move an accepted note to another calendar:

1. In your calendar, locate the note you want to move.
2. Click the check box to the left of the note you want to move, then click Move.
3. Select the calendar where you want to move the note.
4. Click Apply.

   The note is moved to the specified calendar.

To copy an accepted note to another calendar:

1. In your calendar, locate the note you want to copy.
2. Click the check box to the left of the note you want to copy, then click Copy.
3. Select the calendar where you want to copy the note.
4. Click Apply.

   The note is copied to the specified calendar.

Deleting and Undeleting Notes

When notes are deleted from the calendar, they are automatically purged.

IMPORTANT: Use care in deleting already accepted appointments, tasks, and notes. When these items are deleted, you cannot undelete them. The only time that you can undelete an appointment, task, or note, is if it still exists as a deleted item in the INBOX folder.

To delete a note:

1. Locate the note you want to delete from the INBOX folder.
2. Click the check box to the left of the note you want to delete, then click Delete.

   or

   Click the note to open it, then click Delete  .

To undelete a note from the INBOX folder or another folder:

1. Locate the note you want to undelete from the INBOX folder or another folder.
2. Click the check box to the left of the note you want to undelete, then click Undelete.

Managing Mail Messages

This section covers the following tasks:

- "Setting the Mail Message Priority" on page 177
- "Marking a Message As Public or Private" on page 178
- "Marking Mail Messages Read or Unread (Read Later)" on page 178
- "Setting Delivery Status Notification" on page 178
- "Moving and Copying Mail Messages to Folders" on page 179
- "Deleting and Undeleting Mail Messages" on page 179
- "Enabling and Disabling Immediate Purge of Deleted Items" on page 180

Setting the Mail Message Priority

When sending a mail message or when viewing a received mail message, appointment, task, or note, you can set or reset the priority on the item.

You can select High, Normal, or Low, indicating the importance level of the message.

NOTE: When sending a message, you cannot set a priority on appointments, tasks, or notes.

To set the message priority when sending a mail message:

1. Click Compose.
2. In the Message Compose window, click Send Options.
3. Next to Priority, select either High, Normal, or Low.
4. Click Apply.
5. When you are finished writing your mail messages, click Send.

To set the message priority for personal copy on a received mail message, appointment, task, or note:

(Oct. 7, 2003) Still not available on the interface. Is this expected for 3.5? (September 18, 2003) Greg - Yes

1. Click the item you want to change to open it.
2.
3. Click Apply.

4

Marking a Message As Public or Private

(Oct. 7, 2003 - not available) New icon to show how a file is marked (public or private) is under discussion.

When viewing a received mail message, appointment, task, or note, you can mark the item as Public or Private. Marking a message as Public allows those you specify to share your message folder to view the message. Marking a message as Private prevents anyone from viewing the item (including those with shared access) except the mailbox owner.

NOTE: The ability to mark a message public or private works in both private and shared folders. When you mark a message in a shared folder as private, it is the same as moving the message to a private folder. The only one who can access it is the mailbox owner

To mark a received mail message, appointment, task, or note as public or private:

(October 7, 2003) Still not available on the interface. Is this expected for 3.5? (September 18, 2003)Greg - Yes

1. Click the item for which you want to change the status to open it.
2.
3. Click Apply.
4.

Marking Mail Messages Read or Unread (Read Later)

You can mark a message to appear as if it is opened or unopened. For example, if you opened a message and are interrupted, you might want to mark the task as unread to remind you to read it later.

To mark a mail message unread on a received mail message:

1. Locate the mail message you want to mark unread in either the INBOX folder.
2. Click the check box to the left of the mail message you want to mark unread.
3. Select Mark Unread.

   The mail message is marked as unread.

To mark a mail message read:

1. Locate the mail message you want to mark read in either the INBOX folder.
2. Click the check box to the left of the mail message you want to mark read.
3. Select Mark Read.

   The mail message is marked as read.

Setting Delivery Status Notification

Delivery Status Notification notifies you upon successful or failed delivery.

1. Before sending a message, click Send Options.
2. Under Delivery Status Notification, select one of the following options:

- **If Delivery Fails**. Notifies you when a message failed. By default, If Delivery Fails is selected.
- **If Delivery Succeeds**. Notifies you when the message is successfully delivered.
- **On Failure and Success**. Allows you to receive a notification of Failure or Success as available in the previous options.

3 Select Apply.

Moving and Copying Mail Messages to Folders

You can move or copy mail messages to other folders as needed.

NOTE: You can use the Rules feature to move incoming mail messages to a different folder under defined conditions. For more information, see "Using Rules" on page 187.

To move mail messages to other folders:

1 Locate the mail messages you want to move from the INBOX folder.

2 Click the check box to the left of the mail messages you want to move.

3 Select the folder where you want to move the mail messages.

4 Click Apply

The mail message is moved to the specified folder.

To copy mail messages to other folders:

1 Locate the mail messages you want to copy from the INBOX folder.

2 Click the check box to the left of the mail messages you want to copy.

3 Select the folder where you want to move the mail messages.

4 Click Apply

The mail message is copied to the specified folder.

Deleting and Undeleting Mail Messages

When mail messages are deleted, the Delete mark  is placed next to the appointment to indicate it is deleted.The item is not permanently removed from your mailbox, however, until you purge it. As long as an item is not purged, you can still undelete it.

When the mail message is undeleted, the Delete mark  is removed to indicate it is no longer deleted.

To delete a mail message:

1 Locate the mail message you want to delete from the INBOX folder.

2 Click the check box to the left of the mail message you want to delete, then click Delete.

or

Click the mail message to open it, then click Delete.

To undelete a mail message from the INBOX folder or another folder:

1 Locate the mail message you want to undelete from the INBOX folder or another folder.

2 Click the check box to the left of the mail message you want to undelete, then click Undelete.

Enabling and Disabling Immediate Purge of Deleted Items

After you delete a mail message, it is not removed from your mailbox until you purge it. You can set up an immediate purge of deleted messages so you do not need to manually purge items.

NOTE: Appointments, tasks, and notes are automatically purged upon delete.

To enable an immediate purge of deleted messages:

1. Click Options > General Settings.
2. Under Appearance, select Yes for the Purge option.
3. Click Apply.

To disable an immediate purge of deleted messages:

1. Click Options > General Settings.
2. Under Appearance, select No for the Purge option.
3. Click Apply.

Managing Folders

Webmail provides folders to help organize the items you send and receive. When you click Folders and folder name, the contents of the currently opened folder are displayed.

By default, the only folder in the Folder List is INBOX, where messages are stored when you first receive them.

You can add additional folders to further organize your items. For example, you can add a folder to store all messages you receive regarding a specific project you are working on.

This section covers the following tasks:

- "Adding Mailbox or Calendar Folders" on page 180
- "Hiding Folders" on page 181
- "Renaming Folders" on page 181
- "Working with Shared Folders and Calendars" on page 181
- "Setting Up and Removing the Sent Folder" on page 182
- "Deleting Folders" on page 183

Adding Mailbox or Calendar Folders

You can add new mailbox or calendar folders as needed to your mailbox.

1. Click Folders > Create Folder.
2. In the Create Folder field, type the folder name.
3. Select the folder where you want to add a new folder.

   For example, to add a folder inside the INBOX folder, select INBOX. By default, new folders are added at the root level of the mailbox.
4. Select the type of folder you want to add: Mailbox or Calendar.
5. Click Apply.

Hiding Folders

To hide local folders from view or from proxy users:

1. Click Options > Shared Folders.
2. Under Available Folders, click the check box next to the folder that you want to hide.
3. Click Apply.
4. Click Exit  and log in again to WebAccess.

Renaming Folders

You can rename folders as needed.

1. Click Folders > Rename Folder.
2. Select the folder you want to rename.
3. Type a new name for the folder in the New Name of Folder field.
4. Click Apply.

   When you open Folders, the name is changed to the new folder name.

Working with Shared Folders and Calendars

A shared folder is like any other folder, except other people (subscribers) have access to it. For example, if you want to have a place where everyone in your department can store and view items like mail messages, documents, and so forth, you can share a folder. You can create shared folders or share existing personal folders. You choose whom to share the folder with, and what rights to grant each person.

Using shared folders, you can collaborate with team members to easily share all project information and correspondence. One advantage is when new members join the team and are given rights to the team's shared folder; they immediately have all correspondence and background information available for the project.

When subscribers view the contents of the shared folder, they are viewing a local copy. When the shared folder is created, it replicates a copy of the master and copies it to subscribers' local clients. This allows the subscribers to mark and keep track of the items they have read.

When you place a document in a shared folder, subscribers with rights to view the contents of the shared folder do not automatically have rights to edit or add documents. Before they can edit or add documents, the owner of the document has to give them rights.

Four levels of rights exist:

- **Mark Read.** Allows you to mark the item (on your local copy) as read to help you keep track of the opened items.
- **Read.** Allows you to open and view the local copy of the item.
- **Insert.** Allows you to copy an item to the shared folder, which puts the item into the master mailbox. The master mailbox then replicates the item and copies it to the local copy of the shared folder of those with rights to the folder.
- **Delete.** Allows you to delete and purge items from your local copy of the shared folder. The owner of the master mailbox can delete items within the master mailbox, but the delete is not replicated to the local mailboxes. Each individual user must manually delete outdated items.

Shared folders work with IMAP clients, including GroupWise, Ximian Evolution, Microsoft Outlook Express, Microsoft Outlook, Eudora, and Mulberry.

You can also use other features to benefit your team with shared folders. You can set up a personal group in your personal address book that contains all the e-mail addresses for the team members. For more information on the personal groups feature, see "Creating Personal Groups" on page 185.

In addition, you can set up a rule to add any correspondence to the Personal Group to the shared folder. For more information on the rules features, see "Using Rules" on page 187.

To share a folder or calendar with a subscriber:

1. Click Options > Shared Folders.
2. Under Add a Share, select the folder you want to share.
3. Under Add Share for User, type the user names (separated by a semicolon, comma, or space) that you want to give rights to share the folder.
4. Click Apply.

To unsubscribe a remote folder from sharing:

1. Click Options > Shared Folders.
2. Under Folders you are sharing, click Delete next to any user that has rights to view a folder you do not want to share.
3. Click Apply.

To grant or remove rights:

1. Click Options > Shared Folders.
2. Under Folders You Are Sharing, find the user or users you want to grant or remove rights.
3. Click in the Mark Read, Read, Insert, or Delete check boxes to select or deselect rights for users.
4. Click Apply.

To remove user from access to shared folders or calendars:

1. Click Options > Shared Folders.
2. Under Folders You Are Sharing next to the user you want to remove access, click Delete.
3. Click Apply.

Setting Up and Removing the Sent Folder

By default, copies of sent messages are not retained in your mailbox. Saved copies of sent messages occupy space in your mailbox and count against your mailbox quota. You can, however, designate a folder to store copies of sent messages.

NOTE: If you use both an IMAP mail client and Webmail (for example, you use an IMAP mail client on your desktop computer, but you use Webmail on your laptop), create a Webmail folder matching your IMAP mail client's Sent folder. Then, select that folder as your Sent folder in Webmail. Matching the Sent folder names in Webmail and your IMAP mail client enables the folders to synchronize when you switch back and forth between mail systems. Some IMAP mail clients might work differently.

To designate a folder to collect sent messages:

1. Create a new folder to store sent messages. For more information, see "Adding Mailbox or Calendar Folders" on page 180.

For example, create a folder named “Sent Messages.”

2. Click Options > General Settings.
3. Under Appearance, from the Sent Folder drop-down list, select the folder you created.
4. Click Apply.

To disable the folder collecting sent messages:

1. Click Options > Mailbox Management.
2. Under Mailbox Settings, from the Sent Folder drop-down list, select Disable.
3. Click Apply.

Deleting Folders

You can delete an entire folder and its contents.

IMPORTANT: Use care in deleting folders. When a folder is deleted, you cannot undelete it.

1. Click Folders > Delete Folder.
2. Select the folder you want to delete.
3. Click Apply.

Using Address Books

Webmail address books store information about users and organizations that is displayed in HTML format. Using an address book, you can search for contact information to add e-mail addresses to a message, appointment, task, or note you want to send.

Within Webmail, there are three address books. One is to store personal and professional contact information and the other two are both based on LDAP (Lightweight Directory Access Protocol), which is the protocol NetMail uses to access address books.

The administrator gives the user rights to use any of these address books in the ModWeb Mail module. For more information, see “Modular Web Agent Modules” on page 85.

Check with Kristi if this is the right location. Also, check on reference to “ModWeb Mail module” and make is consistent to linked term.

The three types of address books are:

- **Personal Address Book**. Allows you to create new address book entries to store information about your personal or professional contacts.
- **System-Wide Address Book.** Allows you to access a directory of names from within your organization. Your administrator can give you rights to use system-wide address books. The system-wide address book entries are obtained from the messaging server's Address Book Agent.
- **Public Address Book**. Allows a directory of names from the Internet. Your administrator can give you rights to use public address books. Public address book entries are derived from LDAP servers on the Internet (such as the Bigfoot directory service).

Before you can access a system-wide or public address book your administrator has made available, you need to configure a public LDAP Server. For more information, see “Configuring a Public LDAP Server” on page 145.

This section covers the following tasks:

- "Adding Contacts to Items from Address Books" on page 184
- "Searching for Contacts in Address Books" on page 184
- "Adding Contacts to a Personal Address Book" on page 185
- "Creating Personal Groups" on page 185
- "Setting Privacy Settings" on page 186
- "Configuring a Public LDAP Server" on page 186

Adding Contacts to Items from Address Books

You can use the three types of available address books to add contacts to mail messages, appointments, tasks, and notes.

1. Click Compose.

   or

   Click Compose > Appointment, Task, or Note.

2. In the To, CC, or BC fields, add recipients' e-mail addresses, separated by a semicolon, a comma, or a space.

   or

   In the To, CC, or BC fields, click Search to access the Address Book. For more information, see "Using Address Books" on page 183.

3. Click the check box next to the contact name to add the contact as a recipient for the message, then click To, CC, BC to add to the Current Recipients list.

   To remove any contact names from the list, in the Current Recipients list, click check box next to the contact name you want to remove, then click Remove.

4. When finished adding contact names, click Compose to return to the message.

5. Continue to address the message, appointment, task, or note as appropriate, then click Send to send your message. For more information, see "Sending Mail Messages" on page 157, "Scheduling Appointments" on page 163, "Assigning Tasks" on page 169, and "Writing Notes" on page 173.

Searching for Contacts in Address Books

You can search for contacts from the three types of available address books.

To search for contacts in an address book:

1. Click Address Book.

   or

   When composing an item, click Search next to the To, CC, BCC, Required, Optional, or Not Attending fields.

2. Under the Search For field, click the check box by the address book you want to include in the search.

3. Type a first or last name in the Search For field to find a specific contact.

Single-letter search criteria function as wildcards. For example, if you type “J” as the search condition, the search returns all entries beginning with “J.”

The Search For field is not case sensitive. For example, Earl Nelson is the same as earl nelson.

or

Leave the Search For field empty to list all addresses from the personal address book. (Ensure Personal is selected.)

4. Click Search.

   When you click Search, a display of entries appears, matching your search criteria.

5. When the recipient’s name appears, click the check box next to their name and click To, CC, or BCC.

   This adds all the names to the To, CC, or, BCC recipient type accordingly.

6. Click compose to return mail message, appointment, task, or note as appropriate to complete, then click Send to send your message.

   For more information, see “Sending Mail Messages” on page 157, “Scheduling Appointments” on page 163, “Assigning Tasks” on page 169, and “Writing Notes” on page 173.

Adding Contacts to a Personal Address Book

You can add contacts to your personal address book in two ways. You can go directly to the address book and add the contact information or you can open a received message to add a new contact.

To add contacts to a personal address book:

1. Click Address Book.
2. In the Personal area, select Add.
3. Fill in the First and Last Name of the contact you want to add.
4. Type an e-mail address if you want to send messages to the contact.
5. Type information in the other fields as desired.
6. Click Apply.

To add contacts to a personal address book from a received item:

1. From the INBOX folder or other folder, locate the received item from the contact you want to add to your personal address book.
2. Click Add in the From line of the message.

   A window appears allowing you to add a new personal address book entry.
3. Type in any additional information you want to add to any blank fields.
4. Click Apply.

Creating Personal Groups

A group is a list of users you can send messages to by selecting the group name rather than selecting or typing each individual name or address. When you select a personal group as the recipient for a message, appointment, task, or note, all the individuals in the group receive the item.

For example, a manager could create a personal group for all direct reports. The manager could then use the personal group to schedule team meetings, send a task for project status reports, or communicate general information to the team.

To create a personal group:

1. Click Address Book.
2. Under Personal, click Add.
3. In the First Name or Last Name field, enter a name for your personal group.
4. In the E-Mail Address field, enter the e-mail addresses of each individual you wish to include in your personal group. Each address entry can be delimited by either a semi-colon, a comma, or a space.
5. Click Apply.

The personal group now appears in your Personal Address Book. When you select a personal group as the recipient for a message, all the individuals in the group will receive the message.

Setting Privacy Settings

You can choose how much system-wide address book information you want to share with other Webmail users.

NOTE: Depending on how your administrator has configured your system, you might not have access to the Privacy feature.

To set privacy settings:

1. Click Options > General Settings.
2. Under General Settings, use the Privacy drop-down list to select a level of privacy, including the following levels:
   - **None**. All Webmail users are given access to your first and last name, e-mail address, and phone number if this information is available.
   - **Limited**. All Webmail users are given access only to your name and e-mail address.
   - **Unlisted**. No Webmail users are given access to your personal information.
3. Click Apply.

Configuring a Public LDAP Server

If you want to access public address books, you need to configure a public LDAP Server for your personal use. Public address books are derived from LDAP servers on the Internet (such as the Bigfoot directory service).

NOTE: Depending on how your administrator has configured your system, you might not have access to the Public LDAP Server feature.

To configure a public LDAP server:

1. Click Options > General Settings.
2. Under General Settings, provide the host name or IP address of the public directory you want to use in the Public LDAP Server field.
3. Click Apply.

Using Rules

Use rules to define actions that you want automatically performed on the messages, appointments, tasks, or notes you receive or send. Rules can help you organize your Mailbox, automate your Mailbox while you are away, delete unwanted items, and save you time.

Rule actions include:

- **Move To**. Moves an item to the folder you specify. For example, you receive a monthly e-mail newsletter. When the newsletter arrives, you can have a rule move it to a folder to read later.
- **CC To**. Adds a designated address to the CC field. For example, when you receive e-mails about new job openings, you can have a rule automatically forward messages to a personal group of contacts looking for jobs.
- **Delete**. Marks an item you specify as deleted. For example, if you receive messages you do not want from a sender, you can have a rule automatically delete any messages received from that sender.
- **Forward To**. Forwards an item to the recipients you specify. For example, when you are away on vacation, you can have a rule automatically forward specified mail to a co-worker.

You can apply the rule to all new items or only new items that meet your established criteria.

When setting up rules, you define any specified conditions. For example, you might want to move all items you receive from your supervisor to a specific folder. You can define a condition so that only messages with your supervisor's name on the From line are moved to that folder. All other items remain in your INBOX folder.

When setting up the rules, you can move the conditions up or down on the list.The conditions within a rule are executed in preceding order first to last and the rules are executed in preceding order first to last.

This section covers the following tasks:

- "Creating Rules" on page 147
- "Activating and Deactivating Rules" on page 149
- "Deleting Rules" on page 149

Creating Rules

When you create a new rule, you need to do the following:

- Define the information you want the rule to search for before performing an action.

  For example, you can have the rule search for a particular e-mail address.
- Define the action you want the rule to run when the information is found.

  For example, when an incoming message comes into your mailbox that includes an e-mail address that keeps sending you unwanted e-mails, you can set up a rule to automatically delete any e-mails from that e-mail address.

To create a rule:

1. Select Options > Rules.
2. Click the rule type: Move To, CC To, Delete, or Forward To.

3 Click the If drop-down list to define the Message Field option that you want to monitor. (Options include: From, To, CC, Subject, Body, and Apply to All Messages.)

   For example, if you are an assistant to an executive and you want to move all messages you receive on behalf of an executive to a separate folder, select To as the Message Field option you want to monitor.

4 In the Contains field, type information you want to search for in the Message Field you selected in Step 2.

   For example, type your executive's e-mail address.

5 Supply the information you need to perform the action of the rule if the search is successful.

   Do one of the following appropriate for your rule:

   - **Move To:** From the drop-down list of available folders (such as INBOX, MyFolder, Sent Messages, etc.), select the folder where you want the items moved.
   - **CC To:** Type the Internet e-mail address of the contact you want to copy the messages to.

     This action copies all incoming specified items to the specified recipient. It also leaves a copy in your mailbox.
   - **Delete:** This action deletes all incoming specified items. You can always retrieve the deleted items if the items are not purged.
   - **Forward To:** Type the Internet e-mail address of the contact you want to forward the messages to.

     This action forwards all incoming specified items to the specified recipient. It does not leave a copy in your mailbox.

6 If applicable for your rule, select Stop on Match.

   Select the Stop on Match check box when you want to apply the rule to the first item that is found.

7 Click Apply.

Activating and Deactivating Rules

Instead of deleting a rule that you do not want to run, you can deactivate a rule, allowing you to reactivate it for use in the future. When needed, you can reactivate the rule. If you want to delete the rules, see "Deleting Rules" on page 149.

To activate a rule:

1 Select Options > Rules.

2 Click the Active check box to select it next to the rule you want to activate.

3 Click Apply.

To deactivate a rule:

1 Select Options > Rules.

2 Click the Active check box to deselect it next to the rule you want to deactivate.

3 Click Apply.

Deleting Rules

You can delete the rules you create or you can deactivate rules. For more information, see "Activating and Deactivating Rules" on page 149.

IMPORTANT: Use care in deleting rules. When a rule is deleted, you cannot retrieve it.

1. Select Options > Rules.
2. Click Delete next to the rule you want to delete.

Downloading Mail from Other Accounts

If multiple e-mail accounts exist, you can set up WebAccess to routinely retrieve messages from your other accounts.You can also choose to leave copies of your incoming mail on the server, allowing you to access your mail from all your accounts.

This section covers the following tasks:

- "Downloading Mail from Other Accounts" on page 189
- "Enabling and Disabling the Leave on Server Option" on page 190

Downloading Messages from Other Accounts

Mail Proxy is a feature that allows you to retrieve messages sent to other e-mail accounts. For example, if you have e-mail accounts at work, home, and school, you can configure Webmail to copy any new messages from those accounts to your mailbox.

Before configuring your proxy settings, you need to understand the following:

- The e-mail accounts must run on a POP3 or IMAP service. You cannot retrieve mail from Web only services such as Hotmail or Yahoo.
- Message retrieval is not instantaneous. The Proxy service runs at intervals set by your system administrator (every 1, 2, or 3 hours). Updates to your account occur on this preset schedule.
- You can proxy up to three e-mail accounts.
- Some e-mail providers allow access to your mailbox only if you log in within a specified IP address range that belongs to the service. These providers assign you an IP address upon login. In these cases, Proxy does not work even if it is a POP3 or IMAP e-mail service.
- You need to know the Host Name of the POP or IMAP server for your service provider, such as imap.myisp.com, mail.myisp.com, or pop.mail.myisp.com. If you do not know the host name, contact your service provider.

NOTE: Depending on how your administrator has configured your system, you might not have access to download messages from other accounts.

To download messages from other accounts:

1. Click Options > Mail Proxy.
2. In the Host field, type the host name of the POP or IMAP server of your service provider.

   For example, the host name format is imap.myisp.com, mail.myisp.com, or pop.mail.myisp.com. If you do not know the host name, contact your service provider.
3. Type your user name for that account in the Username field.

   For example, lmarshal.
4. Type your password for that account in the Password and Retype Password fields.

For example, password123.

5 From the Type drop-down list, select IMAP or POP3.

For the Proxy feature to work, the POP3 or IMAP service is required for foreign mail accounts.

Also, you cannot retrieve mail from Web-only mail services such as Yahoo or HotMail.

6 If you want to leave copies of your mail in your original mailbox, click the Leave check box.

For more information, see "Enabling and Disabling the Leave on Server Option" on page 190.

7 Click Apply.

Enabling and Disabling the Leave on Server Option

You might want to leave the mail on the server if you are accessing your mail from client other than Webmail. When you enable this option, you do not receive mail from the other client, only from Webmail.

When you leave mail on a server, it takes up server space. Because you are usually allotted a limited amount of space, we recommend that you leave it unselected unless sufficient space exist.

To enable the Leave on Server option:

1 Select the Leave on Server check box.

To disable the Leave on Server option:

1 Select the Leave on Server check box.

Giving Users Proxy Access to Your Mailbox and Calendar

Administrative assistants, co-workers, and others might need to access your mailbox and calendar to manage and process your incoming mail messages, appointments, tasks, or notes.

Two levels of rights exist:

- **Read Only** Allows those granted access to view your mailbox and calendars.
- **Read, Compose, and Delete.** Allows those granted access to view, edit/add, and remove items contained in your personal mailbox or calendars.

NOTE: You can hide some folders and calendars in your mailbox from proxy users. For more information, see "Hiding Folders" on page 181.

To give proxy rights to other users to your mailbox and calendar:

1 Click User Proxy.

2 Under Grant Proxy Rights to Another User, type the username for the person you want to grant rights.

The person is automatically granted Read Only rights.

3 Click Apply.

4 If desired, click the Allow full rights option to give the person Read, Compose, and Delete rights.

To restrict access to previously granted rights:

1 Click User Proxy.

2 Under Users who are allowed to act as proxy for you, click the Restrict Access option.

3 Click Apply.

The person rights are restricted to Read Only rights.

To delete user from proxy access:

1 Click User Proxy.

2 Under Users who are allowed to act as proxy for you, click Delete.

3 Click Apply.

The person is deleted from accessing your mailbox and calendar.

Changing Password and Secret Question/Answer Information

(October 7, 2003) Not available in Webmail. Is this the intent? (September 18, 2003) Greg, no, it should be there. It is also removed from WebAccess and it should be there.

Changing Webmail Settings

This section covers the following tasks:

- "Changing the Timeout Setting" on page 191
- "Changing Language and Encoding Settings" on page 191
- "Changing from Webmail to WebAccess" on page 192
- "Changing Number of Messages Listed Per Page" on page 192
- "Changing the Webmail Page and Font Colors" on page 193

Changing the Timeout Setting

Specific actions, such as opening and item, sending an item, or composing a message without sending it, generate a call to the Web server. Other actions, such as scrolling through items in the item list, or reading Help topics, do not generate a call to the Web server. If, for a period of time, you leave Webmail alone or perform actions that do not generate a call, Webmail logs you out. Doing so not only provides security for your e-mail, but also ensures that the Web server and Webmail run efficiently. When you are logged out, if you attempt to perform an action, you are prompted to log in again.

NOTE: Depending on how your administrator has configured your system, you might not have access modify the timeout setting.

To change the timeout setting:

1 Click Options > General Settings.

2 Under General Settings, type a timeout interval (from 1 to 40 minutes) in the Timeout field.

3 Click Apply.

Changing Language and Encoding Settings

If you are experiencing problems with correct character display in Webmail, verify that the language and character-set encoding are configured properly.

To enable Webmail to display information in the language of your choice, you need to:

- Set the language to ensure that your Webmail language setting matches the language in which you normally receive messages.
- Select the encoding that supports the selected language.

When Webmail receives encoded information, it uses the currently selected character-set definition to display the information. It also uses the character-set definition to encode all outgoing messages. For this reason, you need to ensure that you select the correct character-set encoding for your language.

To change language settings:

1. Click Options > General Settings.
2. Under Appearance, use the Language drop-down list to select your language.
3. Click Apply.

   Language changes are immediately implemented.

To change encoding settings:

1. Click Options > General Settings.
2. Under General Settings, use the Default Charset drop-down list to select the appropriate character-set encoding for your language.

   IMPORTANT: On Windows workstations, Webmail uses Windows encoding to display characters. On other platforms, Webmail uses ISO encoding. If both encoding types are displayed, choose the encoding that is appropriate for your platform.
3. Click Apply.
4. Exit Webmail and log back to implement the changes.

Changing from Webmail to WebAccess

NetMail offers two Web interfaces, WebAccess and Webmail.If your administrator has enabled it, you can use either interface.

To change template settings:

1. Click Options > General Settings.
2. Under Appearance, use the Select Default Template drop-down list to select WebAccess.
3. Click Apply.

Changing Number of Messages Listed Per Page

You can determine the number of messages appearing per Web page inside your various folders. The default number of messages per page is 10. You can choose to display from 5 to 50 messages per page. When messages are spread over multiple pages, click Next to view each successive page.

To change number of messages per page:

1. Click Options > General Settings.
2. Under Appearance, use the Messages Per Page drop-down list to select the number of messages you want to display per page.
3. Click Apply.

Changing the Webmail Page and Font Colors

In Webmail, you can change the page and font colors that appear on the screen.

NOTE: Depending on how your administrator has configured your system, you might not have access modify the Webmail page and font colors.

1. Click Options > General Settings.
2. Under Colors, use the Page, Border, Section, Field Name, and Field Body drop-down lists to customize the colors and fonts that appear in Webmail.

   Click Color Table to view available colors and their color numbers.
3. Click Apply.

Changing Time and Date Settings

This section covers the following tasks:

- "Setting Time Zone Setting" on page 193
- "Setting the Short Date Format" on page 193
- "Setting the Time Format" on page 194

Setting Time Zone Setting

To ensure that dates and times are correct in messages, appointments, and other time-relevant information, you must indicate to Webmail the time zone for your location. The time is then automatically adjusted for appointments sent between people in different time zones.

For example, if you are located in New York and schedule a conference call with people in Los Angeles for 4:00 p.m. your time, the appointment received by the Los Angeles recipients shows the conference call at 1:00 p.m. their time.

For your message to appear with the correct time stamp, you must ensure that your time zone is set correctly.

To change your time zone setting:

1. Click Options > General Settings.
2. Under Appearance, use the Time Zone drop-down list to select the appropriate time zone.
3. Click Apply.

Setting the Short Date Format

(October 17, 2003) You can set a short date, but not the long date. WebAccess allows you to do both. Can you let me know intent for Webmail?

You can change the date format within Webmail.

To change the short date format:

1. Click Options > General Settings.
2. Under Appearance, use the Short Date Format drop-down list to select the format of your choice.
3. Click Apply.

Setting the Time Format

You can change the time format within Webmail.

1. Click Options > General Settings.
2. Under Appearance, use the Time Format drop-down list to select the format of your choice.
3. Click Apply.

8 System Administration

NetMail provides several features that automate or simplify system administration. This section is designed to help you leverage those features to lower your overall IT costs.

Section topics include

- "User E-mail Addresses" on page 195
- "Task-Oriented Management" on page 196
- "User Self-Administration" on page 199
- "Fixing Corrupt Mailboxes" on page 206
- "Limiting the Size of User Mailboxes" on page 206
- "Configuring Multiple User Objects Simultaneously" on page 208
- "Using Local Aliases to Facilitate System Administration" on page 210
- "Fault Tolerance" on page 212

User E-mail Addresses

By default, NetMail agents recognize the Internet E-mail Address attribute in the User object as the user's Internet e-mail address. For example, the Address Book Agent references this property in providing address book information. Likewise, the Modular Web Agent implements the Internet E-mail Address attribute as the user's default Reply To address.

NOTE: NetMail does not verify that the domain listed in the User Object's Internet E-mail Address property is a supported Global or Hosting domain. Therefore, it is recommended you use the Alias Agent to populate this property or manually ensure the domain is valid.

If the Internet E-mail Address property is NOT configured in the User object, NetMail dynamically generates the user's e-mail address as follows:

1. If the user belongs to a Hosting Domain, NetMail simply uses the username as the e-mail address.
2. If the user belongs to a Global Domain, NetMail generates the e-mail address from the username and the user's Internet domain (username@domain).

   To identify the user's Internet domain, NetMail looks in the following objects:

   - **2a** If the user is associated with a Parent object, NetMail looks in the Parent object's Global Domains list.
   - **2b** If no Global Domain is configured in the Parent object, NetMail looks for the user's Container Domain.
   - **2c** If no Container Domain is configured, NetMail uses the messaging server's Official Domain.

Task-Oriented Management

One of the most tedious and time-consuming tasks administrators face is maintaining user accounts. It is much more efficient and cost-effective to off-load this task to the individuals, such as personnel staff members or administrative assistants, who actually manage employee information. However, opening the tree to non-technical staff makes most system administrators uneasy.

With Task-Oriented Management (TOM), NetMail 3.5 virtually eliminates the risk of delegating account management to end-users. Users are only given rights to create, modify, delete, or import accounts in specific domains and contexts. You can even limit the number of accounts that a TOM administrator can add.

Another advantage is that all administrative functions are performed in WebAccess, so the operations are familiar, intuitive, and user-friendly. Users don't need to know anything about eDirectory™ to competently perform their assigned management functions.

All task-oriented management functions are enabled by the Modular Web Agent Task-Oriented Management Module. This module is created under the Modular Web Agent. (See "Creating the Modular Web Agent Modules" on page 85.) While it has no configurable options, the Task-Oriented Management Module must be running to provide TOM functionality in WebAccess.

Task-Oriented Management is actually configured in the Parent and User objects. In the Parent object, you assign which Internet domains and NMAP contexts the TOM administrator can manage. You can also enter custom information (such as instructions or policies) that will display in the TOM administrator interface.

The following table provides an explanation of the Parent object's TOM properties:

Object Description is removed from interface.

Table 4 Parent Object TOM Properties

Option	Function
Task Oriented Management	These properties only apply to TOM administrators associated with the current Parent object. Changes to TOM properties are immediately implemented

Option		Function
	Managed Domain Names	The Hosting Domains which TOM administrators can select when creating new user accounts. The usernames for new Hosting Domain accounts include the selected domain's name (name@hosted_domain). See "Hosting Domains" on page 250 for information on Hosting Domain usernames. If this field is left blank, the domain defaults to the messaging system's Official Domain as defined in the messaging server configuration. Therefore, the default Internet e-mail address for new Global Domain accounts is username@official_domain. However, due to the nature of how Global Domains are handled in NetMail, you can actually address these users at any of the messaging system's Global Domains. See "Global Domains" on page 248 for more information on how Global Domain addressing works. **IMPORTANT:** If you type any domain in this field, NetMail assumes it is a Hosting Domain and all new users are created with a corresponding username (name@hosted_domain). **IMPORTANT:** The TOM module does verify that the listed domains are valid Hosting Domains. To ensure a valid Hosting Domain, you must include the domain in either the SMTP Agent's or the Parent object's Hosting Domains lists. If the Hosting Domain is listed under the Parent object, you must include the parent object in the SMTP Agent's list of NetMail Parent Objects.
	Managed Contexts	The NMAP context(s) in which TOM administrators can create, modify, delete, or import user accounts. If multiple contexts are selected, NetMail equally distributes User objects among the contexts.
	Maximum number of allowed users	The number of users that any TOM administrator can create associated with the current Parent object.

In the User object, you grant specific rights to the domains designated in the Parent object. The following table defines the User object's TOM rights:

Table 5 User Object TOM Rights

Right		Action
Task Oriented Management		
General		
	Parent Objects	The Parent object(s) with which the current TOM administrator is associated. In the WebAccess interface, the TOM administrator is able to create, modify, delete, or import users in the Global or Hosting Domains associated with the selected Parent object(s). User objects are created in the NMAP context(s) designated in the Parent object. (See the Managed contexts property in Table 4, "Parent Object TOM Properties," on page 196.)
Rights		Changes to these properties are immediately implemented.

Right	Action
Allow user creation	The TOM administrator can create User objects in the NMAP contexts listed in the Parent object. If multiple contexts are listed in the Parent object, NetMail equally distributes new User objects between the contexts. In creating the user account, the TOM administrator can select one of the domains listed in his or her Parent object's Managed domain names property. Use this domain to create the new user's Internet e-mail address (username@domain). If the TOM administrator selects multiple domains when creating the user, the User object is created with the first domain name and Alias objects are created with the subsequent domain names. For example, if the TOM administrator selects domains abc.com and 123.com when creating a user account for jotero, the User object is created as jotero@abc.com. The Alias object, jotero@123.com, points to jotero@abc.com. **IMPORTANT:** When creating usernames, do not use extended characters in Internet e-mail addresses or users cannot access the messaging system or receive messages. Make sure to inform TOM administrators not to use extended characters in usernames.
Allow user import	The TOM administrator can import users using comma-delimited ASCII files. The new User objects are created in the NMAP context listed in the Parent object. If multiple contexts are listed in the Parent object, NetMail equally distributes new User objects between the contexts. The first line in the import file is a header row of sorts. It specifies the attributes you are importing and the order you want them to appear in the user records. Of these attributes, the first three are fixed: ◆ For users belonging to Global Domains, attribute 1 is the username. For users belonging to Hosting Domains, attribute 1 is the full e-mail address (username@hosted_domain.com). The TOM module verifies each Hosting Domain before allowing the import. If the TOM administrator doesn't have rights to a given user's domain (for example, if the Hosting Domain isn't listed in the Parent object's Managed domain names property), TOM errors out the import and proceeds to the next user in the list. ◆ Attribute 2 is the surname. ◆ Attribute 3 is the password. Aside from these fixed attributes, the import file can include any data—not just WebAccess-specific attributes. For example, the first line or header row of the import file can appear as follows: Username, Surname, Password, First name, Middle Initial Following the header row are the user records. Each line represents a different user record. The data in each record is delineated by commas and must appear in the order designated in the header row. Using the header row from the previous example, a user record would appear as follows: simon@test.com, Roberts, ih8beets, Simon, T
Allow user deletion	The TOM administrator can delete users from the NMAP context(s) selected in the Parent object. When a TOM administrator deletes a user account, the administrator is also given the option of removing the user's mailbox and all associated directories.

Right		Action
	Enable domain settings	The TOM administrator can define default user attributes. These attributes are applied to all users created or imported in *any* of the domains designated in the Parent object.

When a user with TOM rights logs in to WebAccess, the Administration button  appears on the toolbar. Upon clicking the Administration button, the user is taken to the WebAccess Administration Window. From this menu, the user can add, delete, modify, or import user accounts based on the TOM rights granted in his or her associated User object.

NOTE: For assistance in adding, deleting, modifying, or importing domain accounts, users can refer to WebAccess help.

User Self-Administration

One of the advantages of NetMail is that you can give users rights to perform many self-administration tasks such as changing passwords, configuring mail forwarding and autoreply messages, creating mail proxies, and even defining language, time, and date formats.

User access to these features is managed by enabling or disabling features in the Parent or User objects. For example, if you enable Rules in the Parent object, all users associated with that Parent object are able to configure rules. Likewise, if you mark the Allow User to Change Password option in a User object, that user is able to change his or her password.

For a complete explanation of the Parent object's configuration options, see "Configuring Parent Objects" on page 262. For information on User object configuration, see Table 5, "User Objects," on page 394.

When you give users access to self-administration features, users can then configure those options in the Modular Web client. Although users can only configure NetMail's self-administration features within Webmail or WebAccess, the features function independently of any particular mail client. For example, if a user configures messaging rules, those rules are executed on all inbound messages, regardless of whether the user is using a POP, IMAP, or Modular Web mail client.

Accessing the Self-Administration Options

To access the self-administration features in the Modular Web mail client, follow these steps:

1. At the workstation, launch a standard Web browser.
2. In the browser's address field, type the Modular Web Agent server's hostname or IP address.

   For example: http://192.168.1.1/ or http://ema.com/

   NOTE: If the Modular Web Agent is not using the default HTTP port (port 80 or, on Novell Nterprise Linux Services, port 52080), you must enter a colon and the current port assignment after the server's hostname or IP address. For example: http://192.158.1.1:85/
3. To authenticate to the Modular Web Agent server, type your username and password.
4. Click OK.

   The Modular Web client appears in the browser.
5. In the WebAccess interface, click the Options icon. In the Webmail interface, click Preferences.

From the client configuration menu, you can modify the client options. Each option is described in the following section.

6 When changes are made to an Options page, click Save to save your changes before moving to the next Options page.

Self-Administration Options

From WebAccess or Webmail, users can configure the following options:

NOTE: All self-administration options are presented here; however, users only have access to those options enabled by the system administrator.

The information in this table is written from the user's perspective (in other words, "you" refers to the user) so administrators can distribute this information to their users.

Option	Function
General Settings	
WebAccess Settings	
Change Your Password	
Password	The group of fields under the Change Your Password heading allow you to change your password without having to contact the system administrator or ISP. You simply type your old password once and then type the new password twice. Your new password is required the next time you log in to the Modular Web Agent. If you are on a Novell network, changing your Modular Web Agent password actually changes your network login password. Therefore, your new password is also required the next time you log in to the network. If you access the Modular Web Agent from your ISP and can't see the Password option, one of two things has happened: either your ISP has not given you rights to change your password, or your ISP requires an SSL connection for password changes. If your ISP requires an SSL connection for password changes, you must log in to your ISP using the Secure Sockets Layer (SSL) protocol. To log in to your ISP using SSL, follow these steps: 1. In your Web browser, add the letter "s" after "http" in your Modular Web Agent URL. For example, https://mail.companyx.com 2. Press Enter. 3. When prompted, type your username and password. The Password preference is now available. If you receive an error, you must contact your ISP to find out the port required to make a secure HTTP (HTTPS) connection. Changes to this property are immediately implemented.

Option		Function
	Timeout	The amount of idle time before the user is automatically logged out of the Modular Web client. Specific actions, such as opening or sending an item, generate a call to the Web server. Other actions, such as scrolling through items in the Item List, composing a message without sending it, or reading Help topics, do not generate a call to the Web server. If, for a period of time, you leave the Modular Web client alone or perform actions that don't generate a call, the client logs you out. Doing so not only secures your mailbox, but it also ensures that the Web server and Modular Web client run efficiently. If you attempt to perform a function after you have timed out, the Modular Web client prompts you to log in again. If you are logged out while composing a message, the Modular Web client prompts you with a login dialog when you attempt to send the message or go to another page, If you log in successfully, the client resumes the original session so the message is not lost. You can enter a value (in minutes) between 1 and 40. **IMPORTANT:** To apply Timeout changes, you must log out and then log in again.
	Reply To	The user's preferred reply-to address. If this field is left empty, ModWeb uses the Reply To address configured in the User object. If the Reply To address is not configured in the User object, ModWeb uses the Internet E-mail Address attribute from the User object as the user's Reply To address. If the Internet E-mail Address property is not configured in the User object, ModWeb dynamically generates the user's e-mail address as follows: 1. If the user belongs to a Hosting Domain, ModWeb simply uses the username as the e-mail address. 2. If the user belongs to a Global Domain, ModWeb generates the e-mail address from the username and the user's Internet domain (username@domain). 3. To identify the user's Internet domain, ModWeb looks in the following objects: 4. a.If the user is associated with a Parent object, ModWeb looks in the Parent object's Global Domains list. 5. b.If no Global Domain is configured in the Parent object, ModWeb looks for the user's Container Domain. 6. c.If no Container Domain is configured, ModWeb uses the messaging server's Official Domain. Changes to this property are immediately implemented. **NOTE:** If the Reply To address is configured in both the ModWeb client and the User object, the last setting takes precedence.

Option		Function
	Default Charset	When the Modular Web Agent receives encoded information, it uses the character set defined by the message to decode the information. If the message does not define its charset, it uses the default charset. (Most mail clients define their charsets; however, Hotmail does not.) The Modular Web Agent uses this setting to encode outgoing messages before it sends them to the message queue. The preferred default charset is UTF8. The only time not to use UTF8 is if you regularly communicate with mail systems that do not support UTF8. **IMPORTANT:** The Modular Web Agent converts all messages to UTF8 before it displays them in the browser. Changes to this property are immediately implemented.
	Language	The language the Modular Web Agent client interface is using. Changes to this property are immediately implemented.
	Select Template	Predefined templates that control the appearance of the Modular Web Agent client interface. NetMail 3.5 ships with two client templates—WebAccess and Webmail. **IMPORTANT:** To apply template changes, users must log out and then log in again. The WebAccess template provides standard mail client functionality, calendaring, assigning tasks, and writing notes. Administrators can also use the WebAccess template to delegate NetMail administrative functions such as adding, modifying, and deleting user accounts. (See “Task-Oriented Management” on page 196 for more information.) Webmail is the NIMS 2.5 mail client interface. It provides standard mail client functionality and administrators can use the Webmail interface to give users access to self-administration features like changing passwords and configuring vacation messages. For more information, see “Templates” on page 89.
	Messages per page	The number of mail messages that appear at one time on each page of the Modular Web Agent client interface. Refresh the browser window to view your changes.
Address Book Settings		
	Public LDAP Server	The host name or IP address of the public directory you want to use. Changes to this property are immediately implemented.

Option		Function
	Privacy	The user's level of privacy within the messaging system. The privacy level controls what the Address Book Agent reveals about the user. The privacy options are executed as follows: ◆ **None**: The current user's e-mail address, first name, last name, and full name are returned in address book queries. ◆ **Limited**: Only the current user's e-mail address is returned in address book queries. ◆ **Unlisted**: The current user's personal information is not available. **IMPORTANT:** Changes to this option are implemented when the Address Book Agent regenerates its index. (See "Configuring the Address Book Agent" on page 108 for more information.)
	Time and Date Settings	
	Time Zone	The time zone in which you reside. This option determines the time and date stamp applied to your outgoing messages and calendar events. Refresh the browser window to view your changes.
	Short Date Format	The format for abbreviated dates (in other words, dates displayed only in numbers). The available options are US (*mm/dd/yy*), Europe (*dd/mm/yy*), and Universal (*yyyy/mm/dd*). Refresh the browser window to view your changes.
	Long Date Format	The format for long dates (in other words, dates with the names of months completely spelled out and, in some cases, the name of the day abbreviated). Long dates appear top and center on each page in the WebAccess interface and in the heading of the WebAccess Calendar view. The available options are US (Tue, July 03, 2001), Europe (Tue, 03. July 2001), and Universal (03. July 2001). Refresh the browser window to view your changes.
	Time Format	The time format. The available options are US (12-hour clock with am/pm), Europe (24-hour clock), and Universal (24-hour clock). Refresh the browser window to view your changes.
	First Day of Week	The day you want to appear at the first of each week in the WebAccess calendar. Refresh the browser window to view your changes.
Mailbox Management		
	Mailbox Settings	
	Immediate purge of deleted messages	Activates the Purge feature. If enabled, messages are purged from your mailbox when they are deleted. If Purge is not enabled, deleted messages remain in your mailbox until they are manually purged. Changes to this property are immediately implemented.

Option		Function
	Sent Folder	The folder in which your sent messages are automatically stored. If you use both an IMAP mail client and the Modular Web client (for example, you use Outlook Express on your desktop computer, but you use WebAccess on your laptop when you are traveling), the IMAP client automatically creates a Sent folder in your NetMail mailbox. When you open the Modular Web client, that folder displays in the Folder list. If you select the IMAP client's Sent folder as your Sent folder in the Modular Web client, the folders synchronize when you switch back and forth between mail systems. Changes to this property are immediately implemented. **NOTE:** Outlook Express 5, Outlook 98, and other comparable Internet clients support folder synchronization with WebAccess.
	Forward all new messages	Enables the user to forward incoming messages to another e-mail address. Changes to this property are immediately implemented.
	Keep copy	Keeps a copy of all forwarded messages in the user's NetMail mailbox. If Keep Local Copy is not marked, incoming messages are forwarded and not delivered to the user's NetMail mailbox. Changes to this property are immediately implemented.
	Forward to	The e-mail address where the user's incoming messages are forwarded. Mark Forward Mail to in order to forward the user's incoming messages to the designated e-mail address. Changes to this property are immediately implemented.
	Automatically reply to all new messages	Typically, you use this option when you do not plan to retrieve messages for an extended period of time. For example, if you plan to go on vacation, you can enable this option and create an autoreply message that indicates your scheduled return. This message is then automatically sent to anyone who sends you a message. Changes to this property are immediately implemented.
	Message	The custom message that is sent in response to incoming messages.
	Add signature to outgoing messages	Enables the Signature feature to let you append contact information (or any other information you wish to add) to the end of outgoing messages. Changes to this property are immediately implemented.
	Signature	The information you wish to include in your message signature.

Option		Function
Rules		You can use rules to define actions that you want performed on items you receive. For example, you can forward messages or move messages to folders. Rules can help you organize your mailbox, automate your mailbox while you are away, or delete unwanted items. By default, when you save a rule that you've just created, it is automatically activated. The Rules Agent executes the rule for any new items you receive. It does not execute the rule for any items already received. Changes to this property are immediately implemented. For information about creating, deactivating, and removing rules, see “Using Rules” on page 146 for WebAccess and “Using Rules” on page 187 for Webmail.
Proxy Setting		If you have additional e-mail accounts outside of your NetMail account, you can use the Proxy Agent to routinely collect your messages. For example, if you have an e-mail account at work, home, and school, you can specify the addresses and the Proxy Agent retrieves new messages from those accounts to your Modular Web Agent account. Changes to this property are implemented when the Proxy Agent runs its next cycle. Keep the following in mind about the Proxy feature: ◆ Message retrieval is not instantaneous. The Proxy service runs at intervals set by your system administrator (every 1, 2, or 3 hours). Updates to your account occur on this pre-set schedule. ◆ Some e-mail providers allow access to your mailbox only if you log in within a specified IP address range which belongs to that service. They provide you the IP address upon login. In this case, Proxy does not work even if the e-mail service is POP3 or IMAP compliant. The Proxy Agent must run on a messaging server within the user’s messaging system for this option to function.
	Host Name	The hostname or IP address of your other e-mail account’s mail server (for example, mail.schoolname.edu).
	User Name	Your e-mail account username. This is the name you use to access your e-mail account.
	Password	Your e-mail account password. This is the password you use to access your e-mail account. You must type the password twice to verify it.
	Type	The mail protocol you want to use to retrieve messages from your other e-mail account. You can use either the POP3 or IMAP4 protocols. (Contact your account administrator to determine if there is a preference.)
	Leave on Server	If this option is marked, the Proxy Agent leaves a copy of all retrieved messages in the original e-mail account. If this option is unmarked, the Proxy Agent removes the message from the original e-mail account.
Shared Folders		
	Available Folders	
	Add a share	

Option	Function
Folder	
Add Share for User	
Folders you are sharing	
Mark Read	
Read	
Insert	
Delete	

Fixing Corrupt Mailboxes

If a user's mailbox ever becomes corrupted, you can use a back up to regenerate the mailbox.

To fix corrupt mailboxes:

1 Delete the idx files to regenerate the mailbox.

For more information about idx files, see "Mailbox File Structure" on page 294.

NOTE: For additional troubleshooting information, reference NetMail FAQ (http://www.novell.com/coolsolutions/netmail/features/a_nims_faq_nm.html).

Limiting the Size of User Mailboxes

NetMail enables administrators to more effectively plan and manage server storage space by limiting the size of user mailboxes. You can set Mailbox quotas in the NMAP Agent, Parent object, and User object. The following sections review each of these options.

Setting Mailbox Quotas in the NMAP Agent

The NMAP Agent allows you to manage mailbox quotas for all users within the current NMAP Agent's contexts. Through the NMAP Agent, you can either set the same mailbox quota for all mailboxes on the current messaging server or defer to the User object for individual user quotas. Messages, folders, and calendar items count against the mailbox quota.

The NMAP Agent's mailbox quota settings are explained in the following table:

IMPORTANT: You must restart NMAPD to effect any changes in the mailbox quota properties. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option		Function
Mailbox Quota		
	Per User Mailbox Quotas	Mark this option to require individual user quotas. User quotas are set in the NetMail Configuration page of the User object. For further information on User object configuration, see Table 5, "User Objects," on page 394.

Option		Function
	System-Wide Mailbox Quotas	To set the same quota for all mailboxes on the current messaging server, mark this option and type the maximum mailbox size in the Kbyte field. If you select both Per User and System-Wide Mailbox Quotas, you can set quotas at both levels. While the system-wide quota serves as the default quota for all users in the NMAP Agent's assigned contexts, quotas defined in the User object take precedence. For example, you can set a default, system-wide mailbox quota but still allocate more disk space to specific users such as the messaging server postmaster, system administrators, or VIPs using User object mailbox quotas. **NOTE:** You can also define mailbox quotas at the Parent object level. For more information on Parent object mailbox quotas, see the Mailbox Quota property in Table 3, "Configuring Parent Objects," on page 262.
	Quota Return Message	An optional message that is returned to the sender when the recipient has exceeded his or her mailbox quota. The message notifies the sender that the recipient has exceeded the allotted mailbox quota and cannot receive additional messages. **NOTE:** When users are within 10% of their mailbox quota, they receive a system message notifying them that their mailbox is almost full. The message advises them to delete some messages and warns that when their mailbox is full, all inbound messages are returned to the sender.

Setting Mailbox Quotas in the Parent Object

Mailbox quotas defined in the Parent object function as the default Per-User mailbox quota for all User objects associated with the current Parent object.

IMPORTANT: The Parent object's mailbox quota is *not* enabled unless either the System-Wide or Per User Mailbox Quota option is marked in the NMAP Agent's Options page.

The following table explains the mailbox quota options in the Parent object:

NOTE: Changes to these properties are implemented immediately.

Option		Function
NMAP		
	Mailbox Quota	
	Use parent quota, fallback to user quota	Uses the mailbox quota configured in the Parent object. If no mailbox quota is configured in the Parent object, the setting defers to the mailbox quota defined in the User object.
	Disabled	Disables all mailbox quotas for users associated with the current Parent object. This includes mailbox quotas configured in the Parent object, User object, or NMAP Agent.
	Use user quota, fallback to parent quota	Uses the mailbox quota configured in the User object. If no mailbox quota is configured in the User object, the setting defers to the mailbox quota defined in the Parent object.
	Per-user mailbox quotas	The mailbox quota applied to all users associated with the current Parent object. Type the maximum mailbox size in the kByte field. Messages, folders, and calendar items count against the mailbox quota.

Option		Function
	Quota Return Message	An optional message that is returned to the sender when the recipient has exceeded his or her mailbox quota.The message notifies the sender that the recipient has exceeded the allotted mailbox quota and cannot receive additional messages. **NOTE:** When users are within 10% of their mailbox quota, they receive a system message notifying them that their mailbox is almost full. The message advises them to delete some messages and warns that when their mailbox is full, all inbound messages are returned to the sender.

Setting Mailbox Quotas in the User Object

Individual users' mailbox quotas are defined in the User object's Disk Quota field under the NetMail Configuration page. (See Table 5, "User Objects," on page 394.)

For the defined Disk Quota to take effect, you must mark the Per User Mailbox Quotas option in the NMAP Agent's configuration. Additionally, if the User is associated with a Parent object that has a defined mailbox quota, you must select the Use user quota, fallback to parent quota option in the Parent object before the User object mailbox quota can take effect.

Because the User object's Disk Quota property can override mailbox quotas defined in the NMAP Agent and Parent object, you can use it to allot additional mailbox space to individual users (such as system administrators, the messaging server's postmaster, or company VIPs) on a case-by-case basis.

Configuring Multiple User Objects Simultaneously

To expedite user configuration, (NetWare Administrator) allows you to select multiple User objects and simultaneously configure common properties such as mailbox quotas and Parent objects.

NOTE: WebAdmin does not allow you to configure multiple User objects simultaneously.

To access the Multiple User configuration menu in (NetWare Administrator) ,

Ctrl+click the User objects you want to configure.

Select Object > Details on Multiple Users.

The Multiple User configuration menu appears. Each tab represents a specific object property. From the NetMail Configuration page, you can access common NetMail properties.

NOTE: Only those attributes, which you can commonly apply to multiple User objects, are available in the Multiple Users configuration menu.

Make your changes to the properties.

When finished, click OK to apply your settings.

Multiple User Configuration Options

From the Multiple User Details menu, you can configure the following options:

Option		Function
NetMail Configuration		
	Messaging	
	User Disabled	Excludes the selected users from the messaging system. Though the users might reside in a supported NMAP context, selecting this option prevents the users from sending or receiving mail through NetMail. **NOTE:** This option only affects the NetMail messaging system. It does not disable the User objects in eDirectory.
	Disk Quota (kByte)	The users' mailbox quota. Each user's messages, folders, and calendar items count against his or her mailbox quota. This property overrides the System-Wide Mailbox Quota set in the NMAP Agent. For the Disk Quota to take effect, you must mark the Per User Mailbox Quotas option in the NMAP Agent's configuration or the users' Parent object must defer the mailbox quota setting to the User object. Use the Disk Quota property to allot additional mailbox space on a case-by-case basis (e.g., system administrators, the messaging server's postmaster, or company VIPs).
	Privacy	Sets the selected users' level of privacy within the messaging system. The privacy level controls what the Address Book Agent reveals about the selected users. The privacy options are executed as follows: ◆ **None**: The user's e-mail address, first name, last name, and full name is returned in address book queries. ◆ **Limited**: Only the user's e-mail address is returned in address book queries. ◆ **Unlisted**: The user's personal information is not available.
	Default Timeout	The amount of idle time before the user is automatically logged out of the Modular Web client. Specific actions, such as opening or sending an item, generate a call to the Web server. Other actions, such as scrolling through items in the Item List, composing a message without sending it, or reading Help topics, do not generate a call to the Web server. If, for a period of time, you leave the Modular Web client alone or perform actions that don't generate a call, the client logs you out. Doing so not only secures your mailbox, but it also ensures that the Web server and Modular Web client run efficiently. When you have timed out, and therefore are automatically logged out, and you attempt to perform a function, you are prompted to log in again. If you are logged out while composing a message, NetMail prompts you with a login dialog when you attempt to send the message or go to another page, If you log in successfully, NetMail resumes the original session so the message is not lost. You can type a value (in minutes) between 1 and 40.

Option	Function
Parent Object	The Parent object associated with the selected users. The users “inherit” all options configured in the Parent object unless Use user configuration, fallback to parent configuration is marked in the Parent object. This option gives User object settings precedence over the Parent object. All changes to User object properties are immediately implemented.

Using Local Aliases to Facilitate System Administration

Aliases are usernames that resolve to another account. For example, the alias administrator@abc.com can actually resolve to johns@abc.com.

Local aliases differ by the fact that they are only recognized by the local Alias Agent. This enables you to maintain identical aliases, such as Admin or webmaster, in a single messaging system. (Multiple messaging servers and Alias Agents are required.)

If your system is large enough to require several administrators, webmasters, or other administrative roles, you can use local aliases to facilitate system administration. This is accomplished by defining local aliases for specific roles, such as Admin or webmaster. Users throughout the messaging system can then send messages to these “role aliases,” and the messages are automatically routed to the individuals associated with that alias on the users’ respective messaging servers. For example, if user A on messaging server A sends a message to “admin,” the message is routed to jling whereas, if user B on messaging server B sends a message to “admin,” the message is routed to jmendez.

IMPORTANT: NetMail Aliasing does not work if Verify Recipient Addresses When Accepting Messages is selected in the SMTP Agent configuration. When this option is enabled, the SMTP Agent intercepts messages before they are processed in the message queue; consequently, messages addressed to NetMail aliases are deleted before the Alias Agent can process them. For more information, see the Verify Recipient Addresses When Accepting Messages property in Table 4, “Configuring the SMTP Agent,” on page 91.

The following table outlines the options in the Alias Agent’s Local Aliases page:

IMPORTANT: You must restart MSGALIAS to effect any changes in the Alias Agent’s configuration. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)

Option	Function
Local Aliases	

Option		Function
	Add	To create a local alias, 1. Type an alias in the left field. 2. Type the corresponding e-mail address (replacement string) in the right field. 3. If the replacement string addresses a user in a Global Domain, type only the username. You cannot type the complete e-mail address because the domain portion of Global Domain e-mail addresses is stripped out by the SMTP Agent before the message enters the queue. For more information, see "Global Domains" on page 248. 4. Click Add. The alias appears in the list using the following syntax: *alias* string = *user_name* *For example, if user SJohnsto wants users to send e-mail to SteveJ, the alias reads:* SteveJ = SJohnsto Then when users address e-mail to SteveJ, it is delivered to the SJohnsto mailbox. You could also create an alias such as feedback@company.com that would resolve to a local or remote e-mail address. 5. When you are finished typing aliases, click OK to save the aliases to the Alias Agent's local alias table.
	Remove	To remove an alias, select the alias > click Remove.
	Import	Import local aliases in ASCII format if they use an *alias string =user_name* syntax with a carriage return and line feed (<CR><LF>) between lines. To import local aliases, 1. Click Import. 2. Browse to and select the ASCII file of aliases. 3. Click OK.

The following are the most common errors encountered with local aliases:

- The replacement string does not correspond to a valid username.
- The alias resolves to more than one user.
- The replacement string does not exactly match the username.
- The alias is not an exact match.
- If the user belongs to a Hosting Domain, the replacement string must match the user's full e-mail address (username@hostdomain).
- If the user does not belong to a Hosting Domain, the replacement string does *not* include the domain portion of the user's e-mail address.

For more information on NetMail aliasing and the Alias Agent, see "Managing User Aliases" on page 253.

Fault Tolerance

In NetMail, redundancy and failover support you can implement at two levels: the application level and the hardware level.

Application-level clustering consists of duplicating mail services on multiple servers. Due to NetMail's highly modular architecture and eDirectory replication, critical services can run simultaneously on multiple servers and provide the exact same service. Consequently, you can provide fault tolerance for most mail services at the application level.

The message store is the only NetMail component that you cannot clone at the application level. Because only one NMAP Agent is allowed to service a given user context and its associated mailboxes, *hardware-level clustering* is required to allow users to retrieve their mail if an NMAP server goes down. Hardware-level clustering consists of shared storage and hardware failover and is, typically, very expensive.

NOTE: Configuring more than one NMAP server to service the same user context(s) is not allowed and produces unpredictable behavior in the NetMail system.

Application-level clustering, on the other hand, is relatively inexpensive. It is innate to NetMail 3.5 and does not require specialized hardware. In fact, servers in a NetMail application cluster do not even need to run the same operating system. As an added benefit, using application clustering to provide fault tolerance gives you load balancing because you can have all servers active at all times in a NetMail application cluster. Consequently, application-level clustering is the first choice in building system fault tolerance to use wherever possible.

For more information about system redundancy and failover support, see "Building Fault Tolerance in NetMail" on page 41.

Configuring NetMail to Use Hardware Clusters

The following configuration allows NetMail to use hardware clusters on any platform:

Install the NetMail binaries to all the servers in the cluster.

Ensure that all the cluster servers have a local Directory replica.

Create a Messaging Server object and select one of the Server objects in the cluster as the messaging server's NetWare Host. (This is usually one of the servers that you use in the cluster.)

NOTE: Novell Cluster Services allows you to create a Virtual Server object that represents the cluster. The Virtual Server, however, is not related to an NCP server and does not get the same NetMail attributes. Therefore, do not use it as a NetWare Host.

Create an NMAP Agent and configure it to store the message store (MAIL), the single copy message store (SCMS), and the message queue (SPOOL) on the shared volume.

Create objects for any other NetMail agents that you plan to run on this clustered service.

Configure the Messaging Server object to only use the IP address assigned to the hardware cluster.

By default, NetMail detects its primary IP address and writes it to the Messaging Server object at startup. Other NetMail agents use this IP address when they need a connection to the NMAP agent on the current server. However, in a hardware cluster, the primary IP address changes every time the system fails over. Therefore, clusters use secondary IP addresses so that clients only need to look in one place to find clustered services. When a NetMail messaging server participates in a cluster, configure the cluster's secondary IP address in the Messaging Server object.Then, ensure

that the messaging server is configured not to overwrite the cluster's secondary IP address with the primary IP address at startup.

This is done by entering the cluster's secondary IP address in the Force Server IP Address To field.

NOTE: This option is found under the Advanced button in the Status tab. For more information, see "Configuring the Messaging Server" on page 63.

Configure the DBF directory in the Messaging Server object to use the shared volume.

Before starting NetMail in the cluster start script, load ddb with the -s switch.

The syntax for the -s switch is

`-s:Server_object's_full_NDS_context_name_(DN)`

IMPORTANT: You must include the tree name in the Server object's distinguished name.

For example **`-s:novell_tree.netmail.server1`**

NOTE: The server object's context order is opposite of the standard X.500 syntax. In other words, the context proceeds from root to object.

IMPORTANT: The server designated by the -s switch is the Server object associated with the Messaging Server object in step 3.

The -s switch instructs NetMail to use the designated Server object's configuration, regardless of what server it is really running on. Using the -s switch to load ddb enables the cluster to have only one Messaging Server object in the tree, thereby, eliminating the need to maintain and synchronize multiple Messaging Server objects for each server in the cluster.

NOTE: Novell Cluster Services allows you to create a virtual Server object that represents the cluster. Associating the Messaging Server object with the virtual Server object is an elegant failover solution because rather than referencing a single server's configuration, the start script's ddb line references the configuration assigned to the cluster.

NetWare Cluster Scripts

Sample Start Script

```
mount <shared volume>
ddb -s:<tree_name.container(s).server_object>
add secondary ipaddress 10.10.10.10
ims
```

Sample Stop Script

```
ims unload
delete secondary ipaddress 10.10.10.10
dismount <shared volume>
```

NOTE: In versions before and including NIMS 3.0*x*, do not use the **`IMS Unload`** command in the unload script. Instead, use the following script to stop NIMS on that server before dismounting the shared volume(s):

```
unload webadmin
unload mailcon
unload msgsrv
unload ddb
unload syslogd
```

Unloading NIMS in this manner prevents the dismount of the volume before NIMS is completely down, thereby avoiding a potential abend.

9 Auditing Your Messaging System

In NetMail 3.5, Novell® Nsure™ Audit replaces Syslog as the messaging system logging service. During install, Novell Nsure Audit is automatically configured to write messaging system events to a translated log file. This section provides the basic information you need to manage the auditing system's primary components. For complete documentation, see the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/index.html)

- "System Overview" on page 215
- "Configuring the Platform Agent" on page 216
- "Configuring the Secure Logging Server" on page 218
- "Configuring the Data Store" on page 220
  - "Configuring the File Channel" on page 221
  - "Flushing the File Channel Buffers" on page 222
- "Configuring Other System Channels" on page 222
  - "Configuring the SMTP Channel" on page 223
  - "Configuring the MySQL Channel" on page 224
- "Configuring System Notifications" on page 226
  - "Configuring Notification Filters" on page 227
  - "Configuring Heartbeat Objects" on page 229

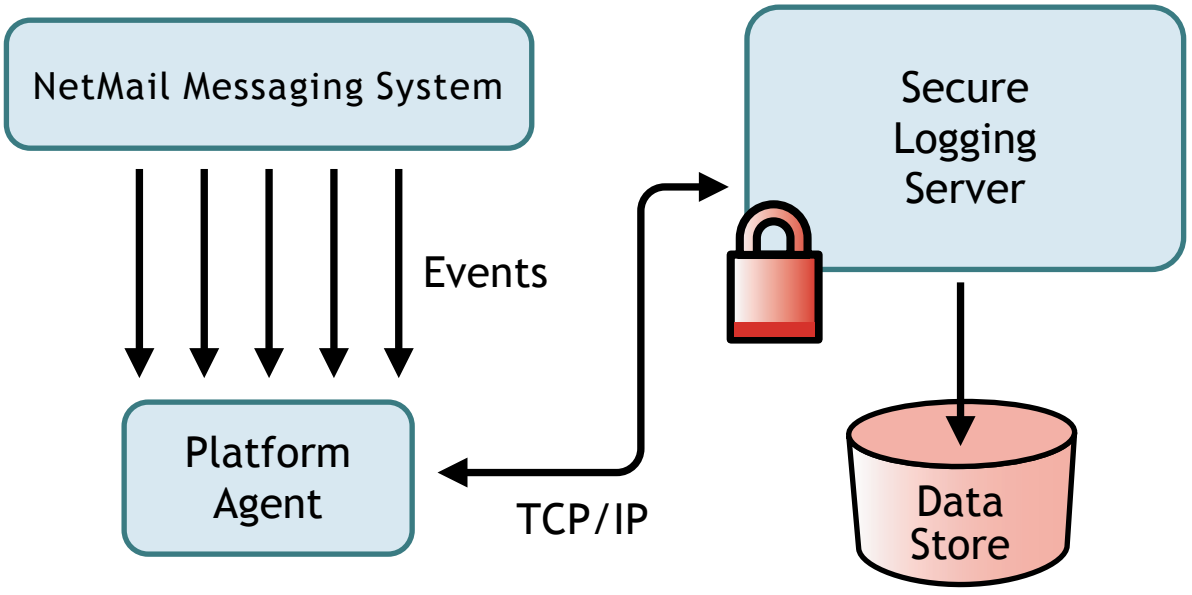
System Overview

Like NetMail, Novell Nsure Audit has a highly modular architecture. Product functions are strategically divided among the following components:

- Platform Agent
- Secure Logging Server
- Data Store

To log events from system applications to the data store, Novell Nsure Audit uses a client/server model. The Platform Agent, as the client piece, receives all log data from the messaging system. It securely transmits this data to the Secure Logging Server which then writes the information to the data store.

Description: Architecture Overview



The following sections review how to configure each of these components.

Configuring the Platform Agent

The Platform Agent, logevent, is the client portion of the Nsure auditing system. It receives logging information and system requests from authenticated applications and transmits the information to the Secure Logging Server.

If the connection between the Platform Agent and the Secure Logging Server fails, NetMail Agents continue to log events to the local Platform Agent just as they always do. The Platform Agent simply switches into Disconnected Cache mode; that is, it begins sending events to the Disconnected Mode Cache until the connection is restored. The switch into Disconnected Cache Mode is completely transparent.

NOTE: The port at which the Platform Agent connects to the Logging Cache Module is configured in the logevent.cfg file. For more information on this parameter, see "Logevent" on page 216.

When the connection to the Secure Logging Server is restored, the cache files are transmitted to the Secure Logging Server.

Logevent

The Platform Agent is not configured through Novell eDirectory™. Instead, the Platform Agent's configuration settings are stored in a simple, text-based configuration file. On NetWare® and Windows systems, the configuration file is logevent.cfg. On Linux* systems, the file is logevent.conf.

The following is a sample logevent.cfg file.

```
LogHost=127.0.0.1
LogCacheDir=c:\logcache
LogCachePort=288
LogEnginePort=289
LogCacheUnload=no
LogReconnectInterval=600
```

```
LogDebug=never
LogSigned=always
```

The entries in the logevent file are not case sensitive; entries can appear in any order; empty lines are legal; and any line that starts with a hash (#) is commented out.

The following table provides an explanation of each setting in the logevent file.

Setting	Description
LogHost	The host name or IP address of the Secure Logging Server that the Platform Agent connects to. If a host name is specified, only the first address associated with that name is used.
LogCacheDir	The path to the Disconnected Mode Cache files. The default log cache directories are as follows: ◆ sys:\etc\logcache\ (NetWare) ◆ \program files\novell\nsure audit\cache\ (Windows) ◆ /usr/naudit/cache/ (Linux) The Platform Agent automatically creates a cache file for each registered application on the current computer. **NOTE:** The filename for each application's cache file is a hash value.
LogCachePort	The port at which the Platform Agent connects to the Logging Cache Module (lcache). The default port is 288. When the Platform Agent initializes, it opens a connection to the logging server and to the Logging Cache Module. Opening both connections at startup enables the Platform Agent to instantly switch to Disconnected Cache Mode if the connection to the logging server becomes unavailable. Although this configuration requires two port assignments, it facilitates faster processing of incoming events because, if the connection to the logging server fails, the Platform Agent doesn't have to block logging applications while it establishes a connection to the Logging Cache Module.
LogEnginePort	The port at which the Platform Agent connects to the logging server. The default port is 289.
LogCacheUnload	The unload setting for the Logging Cache Module. Set the option to "no" if you want to prevent the Logging Cache Module (lcache) from being unloaded. **IMPORTANT:** It is recommended that you do NOT unload lcache. Even if the local logging applications are no longer running, lcache must stay loaded so it can upload cached data to the Secure Logging Server.
LogReconnectInterval	The reconnect interval in seconds. If the Platform Agent loses its connection to the logging server, this is the interval at which the Platform Agent tries to reconnect to the logging server.

Setting	Description
LogDebug	This setting determines how debug events are handled. Set the option to "never" to never log debug events; "always" to always log debug events; and "server" to use the default setting provided by the Secure Logging Server. **NOTE:** In the current version of Novell Nsure Audit, the Secure Logging Server's default LogDebug setting is "always."
LogSigned	This setting determines if logged events are digitally signed. Set the option to "never" to never sign events; "always" to always sign events; or "server" to use the default setting provided by the Secure Logging Server. **NOTE:** In the current version of Novell Nsure Audit, the Secure Logging Server's default LogSigned setting is "never." Digitally signing events creates a non-repudiable log because auditors can determine if an event has been tampered with, deleted, or if the order of events has been changed. For more information, see "Signing Events" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/am8ewzb.html). **IMPORTANT:** The Novell Nsure Audit Starter Pack that ships with NetMail 3.5 chains the first 100 events to allow you to evaluate the product feature. If you wish to fully implement the event signatures, you must upgrade your product license.

The logevent file is stored in the following directories:

Operating System	Path
NetWare	sys:\etc\logevent.cfg
Windows	*windows_directory*\logevent.cfg
Linux	/etc/logevent.conf

Configuring the Secure Logging Server

The Secure Logging Server, the server component in the Nsure auditing system, manages the flow of information to and from the Nsure auditing system. It receives incoming events and requests from the Platform Agents; logs information to the data store; monitors designated events; and provides filtering and notification services.

The Secure Logging Server is configured through the Logging Server object in eDirectory. The Logging Server object is represented in eDirectory as a container with server attributes: it can contain Nsure Audit objects and it stores all the properties and attributes for the Secure Logging Server. Consequently, the server must have access to eDirectory and the Logging Server object before it can launch the Secure Logging Server.

NOTE: To minimize server reaction time and ensure high system performance, you should create a local replica of the Logging Server object and its associated objects on the logging server.

The following table provides an explanation of the Logging Server object's attributes.

Attribute	Description
Configuration	
Host Server	The distinguished name of the NCP Server object associated with the current logging server.
Driver Directory	The directory in which the channel drivers (lgd*) are located. The default channel driver directories are as follows: ◆ sys:\system\ (NetWare) ◆ \program files\novell\nsure audit\ (Windows) ◆ /opt/novell/naudit/ (Linux)
Log Channel	The Channel object the logging server uses to create the central data store.
Secure Logging Certificate File	The path and filename for the Logging Server Certificate. Nsure Audit uses certificates to authenticate client connections. The logging server only accepts connections from applications that have a valid Logging Application Certificate. For general information on how certificates are used in Nsure Audit, see Chapter 11, "Security and Non-Repudiation" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al0lgki.html).
Secure Logging Privatekey File	The path and filename for the Secure Logging Certificate's private key file. If this field is left blank, the logging server assumes the private key is included with the certificate and uses the path and filename for the Secure Logging Certificate. Again, this is only required if you do NOT use the Nsure Audit program's embedded certificates.
Containers	**IMPORTANT:** The logging server only scans these containers at startup. Therefore, if you add a container, you must restart the logging server. For information on restarting the Secure Logging Server, see "Secure Logging Server Startup Commands" on page 320.
Application Containers	The Application containers supported by the current Logging Server object. Application containers provide a reference point through which the logging server can locate Application objects. Application containers must be included in this list for the logging server to locate their associated Application objects. For more information on Application containers and objects, see "Application Objects" on page 15. The Application container in Logging Services is added to this list by default.
Notification Containers	The Notification containers supported by the current Logging Server object. Notification containers provide a reference point through which the logging server can locate Notification Filter and Heartbeat objects. Notification containers must be included in this list for the logging server to locate their associated Notification objects. For more information, see "Configuring System Notifications" on page 226. The Notification container in Logging Services is added to this list by default.
Channel Containers	The Channel containers supported by the current Logging Server object. Channel containers provide a reference point through which the logging server can locate Channel objects. Channel containers must be included in this list for the logging server to locate their associated Channel objects. For more information on Channel containers and objects, see "Configuring Other System Channels" on page 222. The Channel container in Logging Services is added to this list by default.

Attribute	Description
Memory	The memory configuration settings allow you to optimize your logging server's performance. You should adjust these settings based on logging traffic and the amount of memory available to your system. Reasonable values depend on your network. In organizations that require high-performance logging, these parameters should be set high enough to accommodate peak loads. For organizations that must minimize potential data loss, these settings should be very small. While this might slow performance, it minimizes the amount of data that might be lost in the event of server failure. **NOTE:** If incoming log events exceed the amount of memory you have allocated on your logging server, the Platform Agents temporarily write events to their Disconnected Mode Caches until the logging server clears its cache. This prevents any logged events from being lost.
Minimum	The amount of memory the server automatically allocates at boot time to handle logging processes. Because allocating additional memory on the fly can slow down code execution, this setting should represent the minimum amount of memory needed to handle your system's baseline level of logging traffic. Pre-allocating the minimum amount of memory required by your system reduces additional blocking delays when the system is under high load and facilitates faster processing of incoming events.
Normal	The amount of memory the server can immediately allocate if logging traffic exceeds the Minimum memory setting.
Maximum	The maximum amount of memory that can be allocated to logging processes. Setting a maximum prevents Nsure Audit from monopolizing the server's resources. Ideally, this should be set close to the Normal memory setting. If logging traffic exceeds the Normal memory setting, the server incrementally increases the logging cache 4KB at a time. (4KB is the amount of memory required to process a single event.) When the Maximum memory allocation is reached, the server begins dropping Platform Agent connections. If the logging server drops its connection, the Platform Agent simply logs events to its Disconnected Mode Cache, thereby ensuring no information is lost. When free cache is available, the logging server once again accepts Platform Agent connections.
Status	This option allows you to enable or disable the Secure Logging Server. By default, the logging server is enabled. If you mark the Disabled option, you must either restart the server or manually unload the Secure Logging Server for this setting to become effective. Thereafter, the server cannot launch the Secure Logging Server (lengine) until you mark Enabled. For information on unloading the logging server, see "Secure Logging Server Startup Commands" on page 320.

Configuring the Data Store

IMPORTANT: Novell Nsure Audit does not secure the data store. Therefore, to ensure the integrity of your data store, you must manage the security of your log files through the file system.

By default, NetMail 3.5 is configured to write messaging system events to a translated log file. Translated log files can be visually scanned for content; however, you cannot generate reports from these files because there is no consistent field structure—they only contain event descriptions.

The following is a sample from a translated log file:

```
[Sat, 03 May 2003 01:25:10 +0000] eDirInst\Object: A read operation was performed on object
.OntarioTestData.Channels.Logging Services by .Saturn Logging Server.Logging Services
[Sat, 03 May 2003 01:25:10 +0000] eDirInst\Object: A list Subordinate Entires operation has
been performed on container .eDirectory Instrumentation.Applications.Logging Services by
.Saturn Logging Server.Logging Services
```

Configuring the File Channel

NetMail uses the File channel to write messaging system events to the translated log file. The File channel is extremely efficient; it can process over 60,000 events per second on a P4 Xeon class server.

The following table provides a description of the File Channel object attributes. For more detailed information on the File channel, see "File" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al6uwn7.html).

IMPORTANT: You must restart the logging server to effect any changes in Channel object configuration. For more information, see "Secure Logging Server Startup Commands" on page 320.

Attribute	Description
Configuration	
Log File	The path to the log file. The default Log File directories are as follows: ◆ sys:\etc\logdir\ (NetWare) ◆ \program files\novell\nsure audit\logs\ (Windows) ◆ /var/opt/novell/naudit/logs/ (Linux) **IMPORTANT:** All file data stores are named "log." Therefore, if you have multiple File Channel objects, you must point them to different paths.
Purge log files after _____ seconds	The log files' life span. The logging server deletes all log files older than the designated time period.
Roll when log file reaches _____ Bytes	The log file's maximum file size. When a log file reaches the designated file size, lgdfile renames the file and creates a new log file. The archive filename is a combination of the current date and a hexadecimal sequence number (l/yy/mm/dd.###). For example, the first log file archived on July 10, 2003 would be named l030710.001. Subsequent log files archived on the same day would be named l030710.002, l030710.003, etc.
Log Format	The File channel driver can log events in either translated or raw format. Select either Translated or Raw to set the logging mode for the current Channel object.
Translated	This is the default option. In Translated mode, the File channel driver uses the Event ID to look up each event in the application's log schema and it writes the event description to the data store. While a translated log file can be visually scanned for content, no reports can be generated from this file because there is no consistent field structure; it only contains the event descriptions.

Attribute	Description
Raw	In Raw mode, the File channel driver writes the event data in comma-separated format (csv) to the data store. The raw log file is not in a human-readable format; however, they can be imported into spreadsheet programs like Microsoft* Excel.
Translated Language	The language in which events are written to file. **IMPORTANT:** This option is only valid for Translated log files. If logging applications have localized Log Schema files and if those files are added to their respective Application object, the File channel can write Translated log files in the selected language. If there isn't a log schema for the selected language, the channel defaults to English. **NOTE:** You can create parallel logs in multiple languages by defining multiple File Channel objects with different languages and having a single notification filter pass events to all those channels.
Status	This option allows you to enable or disable the Channel object. By default, all Channel objects are enabled. This means that the logging server loads the Channel object's configuration in memory at startup. **IMPORTANT:** The Channel object must be located in a supported Channel container for the logging server to use it. For more information on the logging server's Channel Container property, see "Configuring the Secure Logging Server" on page 218. If you mark the Disabled option, you must restart the Secure Logging Server for the setting to become effective. Thereafter, the logging server cannot load the object's configuration until you mark Enabled. For information on unloading the logging server, see "Secure Logging Server Startup Commands" on page 320.

Flushing the File Channel Buffers

On NetWare, the file channel driver writes events to memory and intermittently flushes the events to disk. The naudit file flush command forces the file channel driver to flush the events in memory to the log file on disk.

To flush the file channel buffers, at the server console enter

```
naudit file flush
```

Configuring Other System Channels

In addition to the File Channel, Nsure Audit also supports several other system channels that can be used to log events or provide system notification. Depending on your system resources and auditing requirements, these channels can be leveraged to log events to databases, send SNMP traps, or e-mail notifications of critical messaging system events.

Novell Nsure Audit currently supports the following channels:


CVR


Oracle (not available on NetWare)


File


SMTP

IMPORTANT: The NetMail™ 3.5 product license authorizes you to use the Nsure Audit program's File, SMTP, and MySQL channels. If you configure and enable the CVR, Java, Oracle, SNMP or Syslog channels, Novell Nsure Audit broadcasts licensing notices every 10 minutes to all your configured channels. (You do not receive notices for an unlicensed channel that is configured, but disabled.) The licensing notice indicates that you should acquire a license when you are done evaluating the additional channels.

Novell Nsure Audit is designed so you can create multiple Channel objects for any given channel driver. This means you can create different channel configurations for different functions or events. For instance, you can configure the Logging Server to use one MySQL Channel object to add events to the central data store and configure a Notification Filter to use another MySQL Channel object to create a filtered log.

You must create Channel objects in Channel containers. The Channel container under Logging Services is automatically created during installation; however, additional Channel containers can be created anywhere in the tree.

Creating Channel objects in the central Channel container under Logging Services is ideal for organizations that need a simple, easy-to-manage logging system. It also suits organizations that are implementing Novell Nsure Audit as an auditing solution and, for security reasons, want to centrally manage their system.

However, if you want to distribute logging system administration, Channel objects can be created anywhere in the tree. For example, if administration is divided by logging server, you can create a Channel container under each Logging Server object.

If you create a Channel container elsewhere in the tree, you must add that container to the logging server's list of supported containers. At startup, the logging server scans its list of supported Channel containers and loads the included Channel object configurations and their associated drivers in memory so it can provide event notification and log events. If a Channel object is not in one of the logging server's supported Channel containers, it cannot be used to provide event notification or log events. For more information on the logging server's Channel Container property, see "Configuring the Secure Logging Server" on page 218.

IMPORTANT: The logging server only loads the Channel object configurations at startup. Therefore, if you create a new Channel container or Channel object, you must first ensure the Channel container is included in the logging server's Channel Container list and then restart the logging server. For information on restarting the logging server, see "Secure Logging Server Startup Commands" on page 320.

The following sections review the configuration settings for the SMTP and MySQL channels. For information on other supported channels, see "Configuring System Channels" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al6t4sd.html).

Configuring the SMTP Channel

The SMTP channel allows the logging server to e-mail logged events. Typically, the SMTP channel is used to e-mail system critical events, such as a server abend, to a system administrator's mailbox, cell phone, or other e-mail enabled device. Using SMTP Channel objects with notification filters, administrators can keep abreast of what is going on in their system as it happens.

The following table provides a description of the SMTP Channel object attributes. For more detailed information on the SMTP channel, see "SMTP" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al6uvnu.html).

IMPORTANT: You must restart the logging server to effect any changes in Channel object configuration. For more information, see "Secure Logging Server Startup Commands" on page 320.

Attribute	Description
SMTP Relay Settings	
Host	The host name or IP address of the SMTP server. If a host name is specified, only the first address associated with that name is used.
User	The user name for the e-mail account the SMTP channel uses to connect to the SMTP server. The user name is only required if SMTP Authentication is enabled on the SMTP server.
Password	The password for the e-mail account the SMTP channel uses to connect to the SMTP server. The password is only required if SMTP Authentication is enabled on the SMTP server.
Message Settings	
Sender	The name that appears in the From: line for all messages sent from this SMTP Channel object. For example, the sender could be `Your Logging Server`.
Recipient	The e-mail addresses to which all events directed through this SMTP Channel object are sent. Multiple recipients are delineated with a comma (,), a space, or a semi-colon (;).
Subject	The text that appears in the Subject line for all messages sent from this SMTP Channel object. The subject line can contain up to 255 characters. This field is optional.
Message	The text that appears in the message body for all messages sent from this SMTP Channel object. The message body can be up to 64KB; however, for performance reasons, this is not recommended. This field is optional.
Status	This option allows you to enable or disable the Channel object. By default, all Channel objects are enabled. This means that the logging server loads the Channel object's configuration in memory at startup. **IMPORTANT:** The Channel object must be located in a supported Channel container for the logging server to use it. For more information on the logging server's Channel Container property, see "Configuring the Secure Logging Server" on page 218. If you mark the Disabled option, you must restart the Secure Logging Server for the setting to become effective. Thereafter, the logging server cannot load the object's configuration until you mark Enabled. For information on unloading the logging server, see "Secure Logging Server Startup Commands" on page 320.

Configuring the MySQL Channel

The MySQL channel allows the logging server to log events to a MySQL database. The logging server can use the MySQL channel to create the central data store or a filtered database.

The space you need for your database depends on a number of factors. These include, but are not limited to, how many events per second you are storing and how long you want to keep the data. The MySQL install, itself, is about 20 MB. (Keep in mind that the MySQL database does not have to be on the same volume as the MySQL binaries.) For the data store, a system that generates around 80 events per second with an average event size of 80 bytes consumes approximately 500 MB of disk space for the database table and 150 MB for the index in a 24-hour period.

NOTE: To enable the MySQL channel, the MySQL client library, libmysql, is installed with the Secure Logging Server.

The following table provides a description of the MySQL Channel object attributes. For more detailed information on the MySQL channel, see "MySQL" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al6uwcj.html).

IMPORTANT: You must restart the logging server to effect any changes in Channel object configuration. For more information, see "Secure Logging Server Startup Commands" on page 320

Attribute	Description
Host	
Address	The IP Address or host name of the database server. If a host name is specified, only the first address associated with that name is used. If the MySQL channel driver loses its connection with the database server, it tries to reconnect every second for 30 seconds. If it cannot reconnect, the driver stores its current events in memory, but it does not accept any new events until the connection is restored. Incoming events are either stored in the Platform Agents' Disconnected Mode Cache (in the case of the central data store) or dropped (in the case of a Notification Filter database).
User	The user account the logging server uses to log in to the database. **IMPORTANT:** In Secure Mode, the default MySQL administrative account, Root, only has rights to log in at the database server. Therefore, if MySQL is running in Secure Mode and you want the logging server to use the Root account to log in to the database, MySQL and the Secure Logging Server must be located on the same server and you must specify a loopback address ("127.0.0.1" or "localhost") in the Address field.
Password	The password the logging server uses to authenticate with the database.
Database	
Name	The name of the database to which the logging server writes events. The default database name is "naudit." The MySQL driver, lgdmsql, automatically creates this database when the logging server first loads the current Channel object configuration in memory.
Table	The database table to which the logging server writes events. The default table is "log." The MySQL driver, lgdmsql, automatically creates this table when the logging server first loads the current Channel object configuration in memory. For information on the default table structure, see "MySQL" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al6uwcj.html).
Advanced	

Attribute	Description
CREATE TABLE Options	This property allows you to customize the default table structure using standard SQL Create Table commands. For example, the `max_rows` and `avg_row_length` commands can be used to increase the maximum size of your table as follows: `max_rows=200000000 avg_row_length=76`
SQL Expiration Commands	This property enables you to use SQL Expiration commands to automate database maintenance. For example, you can automate data archiving by configuring the MySQL channel to automatically save out the current table and create a new table at designated intervals. For a listing of command variables and sample scripts, see "SQL Expiration Command Variables" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al8btmr.html). **HINT:** Use a semi-colon (;) to separate multiple commands that must be executed in sequence. If the commands can be executed in any order, no semi-colon is needed.
Expire at specified time or interval	The frequency at which the expiration command script is executed. For daily regimens, select a time of day. (00 is midnight.) For weekly regimens, select a day of the week. The expiration commands are executed at midnight on that day. For monthly regimens, the expiration commands are executed at midnight on the first day of the month.
Status	This option allows you to enable or disable the Channel object. By default, all Channel objects are enabled. This means that the logging server loads the Channel object's configuration in memory at startup. **IMPORTANT:** The Channel object must be located in a supported Channel container for the logging server to use it. For more information on the logging server's Channel Container property, see "Configuring the Secure Logging Server" on page 218. If you mark the Disabled option, you must restart the Secure Logging Server for the setting to become effective. Thereafter, the logging server cannot load the object's configuration until you mark Enabled. For information on unloading the logging server, see "Secure Logging Server Startup Commands" on page 320.

Configuring System Notifications

Nsure Audit provides two kinds of event notification:

- Filtered Notification
- Heartbeat Notification

Filtered notification tells you when a specific event has occurred; heartbeat notification tells you when an event has not occurred.

As the name implies, Notification Filter objects filter specific events from the stream of incoming events. The filtered events are then routed to one or more channel drivers where they can be logged

to a database or broadcast to an administrator via SMTP. You must create a separate Notification Filter object for every event you want to filter.

Heartbeat objects monitor the stream of incoming events for the occurrence of a specific Event ID. If the event does not occur within the designated interval, the logging server generates a heartbeat event (EventID 0001001). This event is automatically logged to the central data store; however, if you want to receive notification that a specific event has not occurred, you must create a Notification Filter for the corresponding heartbeat event. Unlike Notification Filter objects, a single Heartbeat object can monitor multiple events. In fact, you really only need to create one Heartbeat object in your logging system.

You must create Notification Filter and Heartbeat objects in Notification containers. The Notification container under Logging Services is automatically created during installation; however, additional Notification containers can be created anywhere in the tree.

Creating Notification objects in the central Notification container under Logging Services is ideal for organizations that need a simple, easy-to-manage logging system. It also suits organizations that are implementing Nsure Audit as an auditing solution and, for security reasons, want to centrally manage their system.

However, if you want to distribute logging system administration, Notification objects can be created anywhere in the tree. For example, if administration is divided by logging server, you can create a Notification container under each Logging Server object.

If you create a Notification container elsewhere in the tree, you must add that container to the logging server's list of supported containers. At startup, the logging server scans its list of supported Notification containers and loads the included Notification object configurations in memory so it can filter events, monitor Heartbeat events, and route notifications to the appropriate channels. If a Notification object is not in one of the logging server's supported Notification containers, it cannot use it. For more information on the logging server's Notification Container property, see "Configuring the Secure Logging Server" on page 218.

IMPORTANT: The logging server only loads the Notification object configurations at startup. Therefore, if you create a new Notification container or Notification object, you must first ensure the Notification container is included in the logging server's Notification Container list and then restart the logging server. For information on restarting the logging server, see "Secure Logging Server Startup Commands" on page 320.

Configuring Notification Filters

Notification Filter objects define event criteria and designate which Channel objects should be used to provide event notification.

To define Notification Filters, you must be familiar with the structure of NetMail events. All events have a fixed set of fields. They include:

Event ID	Value 1
Severity	Value 2
Component	Data
Text 1	Group
Text 2	Source IP

NOTE: For more information on event fields, see "Event Structure" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al9m3w5.html).

When you define a Notification Filter, you specify a value for a given event field. To narrow the results, you can define values for multiple event fields. Using standard “and,” “or,” and “not” operators, you can define up to 15 event conditions.

After you define the event criteria, you must select a notification channel. Notification channels are simply the Channel objects the logging server uses to provide event notification. For example, if you want to e-mail events to your mailbox, you must select an SMTP Channel object that is configured to relay events to your e-mail address. Similarly, if you want to log events to a MySQL database, you must select a MySQL Channel object that is configured to write events to the correct database and table. You can define multiple notification channels for any given Notification object.

The following table provides a description of each Notification Filter attribute.

IMPORTANT: You must restart the logging server to effect any changes in Filter object configuration. For more information, see “Secure Logging Server Startup Commands” on page 320.

Attribute	Description
Description	This field allows you to enter a description and any necessary explanation for the Notification Filter. The field limit is 255 characters.
Rule	The Rule defines the filter criteria.
Event Field	The event field on which the logging server filters events. For more information on the event fields, see “Event Structure” in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al9m3w5.html).
Condition	The condition under which the logging server applies the Value to the Event Field. Depending on the Event Field, you can select one of the following conditions from the drop-down list box: ◆ matches ◆ Is less ◆ Is more ◆ is between ◆ contains
Value	The value for the designated Event Field. The logging server applies the Value to the designated Event Field under the defined conditions. If an event matches the criteria, it is sent to the designated notification channel.
Operator	To narrow the filter results, you can define values for multiple event fields. Using standard “and,” “or,” and “not” operators, you can define up to 15 event conditions. The conditions are accumulative; that is, the logging server applies the first condition, then the second, then the third, etc., to progressively narrow the results.
Notification Channels	The Channel objects the logging server uses to provide event notification. You can select multiple notification channels for any given Filter object.

Attribute	Description
Status	This option allows you to enable or disable the Notification Filter. By default, all Notification Filters are enabled. This means that the logging server loads the filter's configuration in memory at startup. **IMPORTANT:** The Notification Filter object must be located in a supported Notification container for the logging server to use it. For more information on the logging server's Notification Container property, see "Configuring the Secure Logging Server" on page 218. If you mark the Disabled option, you must restart the Secure Logging Server for the setting to become effective. Thereafter, the logging server cannot load the object's configuration until you mark Enabled. For information on unloading the logging server, see "Secure Logging Server Startup Commands" on page 320.

Configuring Heartbeat Objects

Heartbeat objects define which Event IDs the logging server is looking for and the interval at which those events must occur. You can also define the information that is returned in the heartbeat event's Text1, Text2, Value1 and Value2 fields.

If an event does not occur within the designated interval, the logging server generates a heartbeat event (EventID 0001001). The information in the Heartbeat object's Text1, Text2, Value1, and Value2 fields is used to populate the corresponding fields in the heartbeat event.

The heartbeat event is automatically logged to the central data store; however, if you want to receive notification that a specific event has not occurred, you must create a Notification Filter for the corresponding heartbeat event.

NOTE: The Notification Filter can differentiate heartbeat events based on the values you define in the Text1, Text2, Value1, and Value2 fields.

The following table provides a description of each Heartbeat object attribute.

IMPORTANT: You must restart the logging server to effect any changes in Heartbeat object configuration. For more information, see "Secure Logging Server Startup Commands" on page 320.

Attribute	Description
Description	This field allows you to enter a description and any necessary explanation for the Heartbeat object. The field limit is 255 characters.
Event ID	The Event ID you want the logging server to monitor. **NOTE:** The Event ID uniquely identifies each type of logged event. For more information, see "Event Structure" in the Nsure Audit 1.0 Administration Guide (http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/al9m3w5.html). If a logging application does not log the Event ID within the designated interval, the logging server generates a heartbeat event. **IMPORTANT:** The Event ID is not included in the heartbeat event. Therefore, you should enter information in the Text1, Text2, Value1, and Value2 fields that allows you to determine which event triggered the heartbeat event.

Attribute	Description
Interval	The maximum number of seconds between each event occurrence. If the event does not occur within the designated interval, the logging server generates a heartbeat event.
Text1	The information that appears in the heartbeat event's Text1 field. It can contain any text string up to 255 characters. **IMPORTANT:** To facilitate filtering of heartbeat events, the Text1, Text2, Value1, and Value2 fields should include information that allows you to identify which event triggered the heartbeat event.
Text2	The information that appears in the heartbeat event's Text2 field. It can contain any text string up to 255 characters.
Value1	The information that appears in the heartbeat event's Value1 field. It can contain any numeric value up to 32 bits.
Value2	The information that appears in the heartbeat event's Value2 field. It can contain any numeric value up to 32 bits.
Operators +-	Click the plus sign (+) to add a new line. Click the minus sign (-) to remove a line. Each line defines a separate event for the logging server to monitor. If a given event does not occur, the logging server generates a unique heartbeat event using the information from the Text1, Text2, Value1, and Value2 fields. There is no programmed limit to the number of events that can be added to Heartbeat objects.
Status	This option allows you to enable or disable a Heartbeat object. By default, all Heartbeat objects are enabled. This means that the logging server loads the object's configuration in memory at startup. **IMPORTANT:** The Heartbeat object must be located in a supported Notification container for the logging server to use it. For more information on the logging server's Notification Container property, see "Configuring the Secure Logging Server" on page 218. If you mark the Disabled option, you must restart the Secure Logging Server for the setting to become effective. Thereafter, the logging server cannot load the object's configuration until you mark Enabled. For information on unloading the logging server, see "Secure Logging Server Startup Commands" on page 320.

10 Securing Your System

One of the foremost concerns in configuring an Internet messaging system is security. Because the Internet is an open, unregulated forum, you must protect your private messaging system from misuse. This section reviews specific options that you can implement to secure client/server communications and protect your system from attack.

Section topics include

- "Setting Up TLS and SSL" on page 231
- "Authenticating SMTP Connections" on page 231
- "Protecting Your System from UBE" on page 233
- "Preventing Others From using Your System to Relay UBE" on page 238
- "Providing AntiVirus Protection" on page 240
- "Managing User Privacy" on page 243
- "Connection Manager" on page 243

Setting Up TLS and SSL

TLS and SSL connections are not supported in Hamachi Beta 2.

Authenticating SMTP Connections

By default, POP3 and IMAP mail clients must always authenticate their users with the mail server before they access the users' mailboxes. However, mail clients do not automatically need to authenticate their users before sending messages through the mail server.

For this reason, SMTP connections pose a potential security risk to Internet mail systems. If a mail system does not require some SMTP authentication, outside users can use the mail server to relay messages. Such is the case with SPAM. Unauthorized users gain access to a mail server and "pirate" the server's resources to relay SPAM messages.

NetMail's SMTP Agent provides two options to secure SMTP connections:

- SMTP Authentication
- SMTP-after-POP

These options are discussed in the following sections.

SMTP Authentication

The most obvious way to secure SMTP connections is to require SMTP authentication. The Only allow remote sending for authenticated senders option in the SMTP Agent's UBE Relaying page enables SMTP authentication. If selected, the e-mail client must authenticate through the ESMTP protocol before the SMTP Agent relays its messages to remote recipients. Netscape Communicator and Outlook Express support ESMTP authentication.

When authenticating users to send remote messages, the SMTP Agent compares the username in the message header to the user's username and password in the NMAP Agent context list maintained by the messaging server. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in the Internet Services container. If the user is not listed in the context list, the SMTP Agent does not accept the user's connection. For more information on the context list, see the Context property in Table 3, "Information Needed When Creating an NMAP Agent Object," on page 68.

If both SMTP-after-POP and SMTP authentication are enabled, they function as an either/or option. If a mail client does not authenticate via POP or IMAP when downloading mail, it must authenticate via ESMTP before it can send remote messages.

NOTE: Netscape Communicator 4.0 automatically tries to authenticate users before sending messages via SMTP, regardless of whether SMTP authentication is enabled on the server. You must manually configure Internet Explorer and previous versions of Netscape Communicator to support SMTP authentication.

SMTP-after-POP

SMTP-after-POP is a back door approach to SMTP authentication. Instead of requiring users to authenticate via the SMTP protocol, it requires users to authenticate with the mail server via their POP3 or IMAP client before sending remote messages. This works for most Internet e-mail clients because e-mail clients always check for e-mail (log in) just before sending messages.

By leveraging the user's POP or IMAP authentication with the messaging server, administrators avoid having to configure users' e-mail clients to support SMTP authentication.

This feature also includes, in the message header, the username of the person who authenticated with the messaging system. This helps track spammers who authenticate with a valid username but fake the message header to mask their identity.

The SMTP-after-POP option requires Connection Manager. Connection Manager tracks users that have authenticated via POP or IMAP. When a user tries to send a message through the SMTP Agent, the Connection Manager Agent verifies that the user has previously authenticated with the messaging server via POP or IMAP. The basic process is as follows:

Table 4 SMTP-after-POP

Stage	Icon	Description
1	 User	When a user logs in to your NetMail system by way of a POP3 or IMAP4 e-mail client, the POP or IMAP Agent sends the username and the client's IP address to the Connection Manager that is configured on the Messaging Server object via UDP port 689.

Stage	Icon	Description
2	 Connection Manager	The Connection Manager stores the username and IP address for a configurable amount of time.
3	 User	Later, the user tries to send a message to a user who is outside the local NetMail system.
4	 SMTP Agent	When the SMTP Agent receives the outgoing message, it queries the Connection Manager configured on its Messaging Server object to verify that the sender's IP address is valid.
5	 Connection Manager	The Connection Manager checks its list of valid IP addresses: ◆ If the sender is identified as a valid user, the Connection Manager confirms that the SMTP Agent can send the remote message and the SMTP Agent transfers the message out of the NetMail system. ◆ If the sender's IP address is no longer recognized by the Connection Manager, the user is required to re-authenticate to the NetMail system by way of POP3 or IMAP4 before he or she can send remote messages.

For specific information on creating and configuring Connection Manager, see "Connection Manager" on page 243.

Protecting Your System from UBE

Unsolicited bulk e-mail (UBE), or SPAM, is one of the most pervasive problems in Internet messaging systems. Receiving these mass mailings wastes your messaging server's resources and it consumes valuable server space in your users' mailboxes.

To help protect your system from UBE, NetMail provides several UBE blocking features. First there is the AntiSpam Agent. This agent blocks messages from specific domains or e-mail addresses. Secondly, there are several anti-SPAM options in the SMTP Agent's UBE Blocking page. Finally, the NMAP Agent's Bounced Message Control feature protects your messaging server and keeps it running efficiently from an abundance of return messages from a UBE mailing. The following sections provide more details on these features.

AntiSpam Agent

Description: AntiSpam Agent icon

The AntiSpam Agent allows the Postmaster or NetMail administrator to build a blackout list of undesirable e-mail domains and addresses. Messages sent from domains and e-mail addresses contained in the blackout list are not accepted into your NetMail system.

Creating an AntiSpam Agent Object

To create the AntiSpam Agent, select the messaging server on which you want to create the agent and choose AntiSpam Agent from the Create menu.

In creating the AntiSpam Agent object, you are prompted for the following information:

Option	Function
Store to be monitored	The Store to be monitored is the message queue serviced by the AntiSpam Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AntiSpam Agent can monitor multiple message queues. However, you can only select one monitored queue when creating the Autoreply agent. You can add multiple monitored queues when configuring the agent.

After you create the AntiSpam Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the AntiSpam Agent

From the AntiSpam Agent's Details menu, you can configure the following options:

IMPORTANT: You must restart ANTISPAM to effect any changes in the AntiSpam Agent's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Table 5 Configuring the AntiSpam Agent

Option		Function
Blocked Sites		
Configuration		
	Blocked Domains and Addresses	A blackout list of domains and e-mail addresses. Messages from these domains and e-mail addresses are removed from the designated message queues.
	Add	To add a domain or e-mail address to the Blocked list, 1. Type a domain or e-mail address In the Blocked Sites box. For example *company.com* or Joe@*company.com*. If you type a domain name, all e-mail addresses ending with that domain are blocked. If you type a specific e-mail address, only that exact address is blocked. 2. Click Add.
	Remove	To remove a domain or address from the Blocked list, 1. Select the domain or address. 2. Click Remove.

Option		Function
	Import	You can import domains and e-mail addresses in ASCII format. You must separate each domain or e-mail address with a carriage return and line feed (<CR><LF>). To import domains and e-mail addresses, 1. Click Import. 2. Browse to and select the ASCII file of domains and e-mail addresses. 3. Click OK.
	Send Back	Returns blocked messages to their senders with the message, “Mail from <*user or domain*> is blocked from this site.”
	CC Postmaster	Copies the postmaster on blocked messages that are returned to their senders. This option works in conjunction with Send Back.
Monitored Queues		A monitored queue is the message queue serviced by the AntiSpam Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AntiSpam Agent can monitor multiple message queues. Use the Browse button to select one or more monitored queues. **NOTE:** You cannot configure multiple AntiSpam Agents to monitor the same queue. Only one AntiSpam Agent can monitor each queue. To verify that an AntiSpam Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the AntiSpam Agent is listed as an NMAP client.
Status		By default, the AntiSpam Agent is enabled. To disable the AntiSpam Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the AntiSpam Agent at startup. However, to immediately disable the agent, you must manually unload ANTISPAM.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317. After the AntiSpam Agent is disabled, the messaging server does not launch ANTISPAM.NLM again until you deselect the Disable Agent option and restart the messaging server.

SMTP Agent UBE Blocking Options

Because it is the first point of contact with inbound messages, the SMTP Agent is a logical filter point for UBE. The following options in the SMTP Agent’s UBE Blocking page help protect your system against UBE. If a message meets any of the selected criteria, it is deleted from the message queue.

Table 3 SMTP Agent UBE Blocking Options

Option		Function
UBE Blocking		This page provides options that block incoming messages from specified sites. These options are designed to protect your messaging system from unsolicited bulk e-mail (UBE) or SPAM. Changes to these properties are implemented within 5 minutes.
Flags		
	Do Not Allow Access from Hosts in Blocked List	Restricts access to your messaging system. If marked, the SMTP Agent refuses connections from any mail host with an IP address designated in the Blocked Hosts list.
	Deny Access to Hosts Not in DNS	Provides reverse DNS lookups. When receiving messages from external systems, the SMTP Agent verifies that the host's IP address and domain correspond to its DNS record. If they don't match, the SMTP Agent drops the connection. **NOTE:** You must configure your DNS server to support reverse DNS lookups for this option to function.
	Override with Authentication	This option provides an exception to the Deny Access to Hosts Not in DNS option. If marked, hosts that are not listed in DNS are given the opportunity to authenticate with the SMTP Agent before their connection is dropped.
RBL Check		Enables the SMTP Agent to do lookups on the Realtime Blackhole List (RBL*). RBL maintains a list of confirmed spammers and open relays. If the mail host matches an entry on the RBL, the connection is refused. To enable this option, mark Perform Check.
	Add	To add an RBL site, type the IP address or host name of the RBL list server and click Add. The RBL entry can include a trailing semi-colon (;) and subsequent text. The text following the semi-colon is displayed as part of the protocol reply informing the sender he is blocked. The following configuration entry references bl.spamcop.net as the RBL Host and then adds a message directing the sender to the SpamCop web site: bl.spamcop.net;You have been blackholed by spamcop.net. Please see http://spamcop.net to get removed If the character sequence *%d.%d.%d.%d* is provided as part of the text, it is replaced by the IP address of the blocked system. Use this feature to generate responses containing URLs that point directly to the RBL system's look-up page. For example, in this configuration entry, bl.spamcop.net;Please see http://spamcop.net/w3m?action=checkblock&ip=%d.%d.%d.%d http://spamcop.net/w3m?action=checkblock&ip is the URL format for SpamCop's lookup page and *%d.%d.%d.%d* generates the IP address of the blocked host. The resulting protocol reply includes a URL that takes the blocked sender directly to SpamCop's lookup page and tests his or her IP address. **IMPORTANT:** If a percent sign (%) is provided as part of the SMTP message text, type it as %%. Using a single percent sign without the letter "d" might crash the SMTP Agent.

Option		Function
	Delete	To remove an RBL site, select the site in the RBL list and click Delete.
	Blocked Hosts	A list of blocked IP address ranges. If Do Not Allow Access from Hosts in Blocked List is marked, the SMTP Agent refuses connections from any host within the designated IP address range. Listing ranges of registered IP addresses blocks specific external hosts from sending mail to or relaying mail through your messaging system. For example, you can choose to list the IP addresses registered to public mail systems (such as Hotmail, Yahoo, and Juno) because spammers frequently use these systems to relay UBE. You can also use this option to block internal hosts. By listing ranges of internal IP addresses, you can block specific workstations from sending any messages over the Internet.
	Add	To add a range of IP addresses to the Blocked Hosts list, 1. Type a range of disallowed IP addresses. For example: 251.70.2.53-251.70.2.60 2. Click Add. Repeat for each additional range of disallowed IP addresses. If you are using WebAdmin, provide only one range per line.
	Delete	To delete a range of IP addresses from the Blocked Hosts list, 1. Select the range. 2. Click Delete.

NMAP Agent Bounced Message Control

The Bounced Message Control feature found on the NMAP Agent's Options page sets a threshold for the number of bounced messages NMAP can process within a set number of seconds. If the number of bounced messages exceeds the defined threshold, the messages are deleted and not processed.

It is a common practice for spammers to falsify the From field in their message so the resulting bounced messages go to a mail server other than their own. Unfortunately, the server that actually owns the domain specified in the From field is inundated with thousands of bounced messages in a short period of time.

The Bounced Message Control feature enables you to keep your NetMail system from wasting system resources during such attacks.

Table 3 NMAP Agent Bounced Message Control

Option		Function
Options		
	Bounced Message Control	Changes to these properties are effective within 5 minutes.
	CC Postmaster	Mark this option to send the Postmaster a copy of bounced messages.

Option		Function
	Limit Bounces To	Select this option to turn on Bounced Message Control. ◆ **Interval**: The time frame threshold (in seconds). ◆ **Entries**: The number of bounced messages NMAP can process during the *Interval* time frame. If the number of bounced messaged exceed the *Entries* threshold within the *Interval* time frame, NMAP deletes the messages.
	Entries	
	Interval	
	Forward Local Undeliverable Messages	

Preventing Others From using Your System to Relay UBE

While inbound UBE is a significant problem, the greater threat to Internet messaging systems is having unauthorized users relay outbound UBE messages through your mail server. This not only affiliates your messaging system with undesirable e-mail, but it wastes your server's resources both in sending the messages and in handling the thousands of bounced messages that come back from invalid e-mail addresses.

The following options in the SMTP Agent's UBE Relaying page prevent your messaging server system from spammers using it to relay UBE. If a connection does not meet the selected criteria, it is dropped.

Table 4 Preventing Others From using Your System to Relay UBE

Option		Function
UBE Relaying		This page provides options that prevent your messaging system from spammers using it to relay unsolicited bulk e-mail (UBE) or SPAM. Changes to these properties are implemented within 5 minutes.
Flags		
	SMTP-after-POP	Prohibits users from sending remote messages through the SMTP Agent until they have first authenticated with the messaging system via their POP3 or IMAP4 client. This works for most Internet e-mail clients because these clients always check for e-mail (log in) just before sending messages. This feature also includes, in the message header, the username of the person who authenticated with the messaging system. This helps track spammers who authenticate with a valid username but fake the message header to mask their identity. SMTP-after-POP requires that you run the Connection Manager Agent and that you configure the Conn. Mgr. option on the messaging server running the SMTP Agent. See "SMTP-after-POP" on page 232 for detailed instructions on configuring SMTP-after-POP authentication.

Option		Function
	Only Allow Remote Sending for Authenticated Senders	Enables Extended SMTP (ESMTP) authentication. If selected, the e-mail client must authenticate through the ESMTP protocol before the SMTP Agent relays its messages to remote recipients. Netscape Communicator and Outlook Express support ESMTP authentication. If both SMTP-after-POP and ESMTP authentication are enabled, they function as an either/or option. If a mail client does not authenticate via POP or IMAP when downloading mail, it must authenticate via ESMTP before it can send remote messages.
	Require Sender to Be in Allowed List for Remote Sending	Restricts access to your NetMail system by selectively allowing access. If marked, only mail hosts with an IP address designated in the Allowed Hosts list can relay remote messages through the current SMTP server. If SMTP-after-POP, ESMTP authentication, and Require Sender to Be in Allowed List for Remote Sending are all enabled, they function as an either/or option. If an e-mail client does not authenticate using of POP or IMAP when downloading mail, it must authenticate using ESMTP or the Allowed Hosts list must include it before it can send remote messages.
	Maximum Number of Recipients per mail	Restricts the number of users who can receive the same message. This option affects both inbound and outbound Internet messages. If a message exceeds the threshold, the SMTP Agent begins at the top of the recipient list and sends the message to the number of recipients designated in this field. You can also configure the ModWeb Mail Module in the Modular Web client to restrict the number of recipients per message sent by users. For information, see “Configuring the Mail Module” on page 86.
Relaying		
	Allowed Hosts	A list of allowed IP address ranges. If Require Sender to Be in Allowed List for Remote Sending is selected, only hosts that fall within the designated IP address ranges are allowed to send messages to remote recipients via the current SMTP Agent. 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. In addition to preventing external hosts from relaying messages through your messaging system, you can use the Allowed Hosts list to prevent internal hosts from relaying remote messages. To restrict which workstations outside your organization that you allow to send remote messages, designate ranges of internal IP addresses. **NOTE:** If a workstation’s IP address is not in an Allowed Hosts range, you can still use the workstation to send messages to users within the local messaging system.

Option		Function
	Add	To add a range of IP addresses to the Allowed Hosts list, 1. Type a range of allowed IP addresses. For example: 251.70.2.53-251.70.2.60 2. Click Add. Repeat for each additional range of allowed IP addresses. If you are using WebAdmin, provide only one range per line.
	Delete	To delete a range of IP addresses from the list, 1. Select the range. 2. Click Delete.
	Relayed Domains (ETRN)	ETRN Domains are messaging systems that use a hosting service, such as an ISP or ASP, to send and receive messages over the Internet. These systems have their own messaging servers, agents, and mail directories; however, all their messaging services are local. Consequently, they must use a hosting service to send and receive remote messages. In most instances, ETRN Domains have non-persistent dial-up connections to their ISP or ASP. For more information on ETRN Domains, see "Servicing ETRN Domains" on page 251.
	Domain(s)	The current SMTP Agent services the ETRN Domains. To support these domains, you must click the Accept ETRN option in the Options page.

Providing AntiVirus Protection

The NetMail AntiVirus Agent integrates with McAfee NetShield*, Computer Associates InoculateIT*, and Symantec CarrierScan* virus engines to provide virus scanning on messages handled by NetMail.

If a message contains a virus, the AntiVirus Agent immediately deletes it from the message queue. You can configure the agent to return the message to the sender with a notice indicating which virus the message contained. It can also send a virus alert to the message recipient(s) indicating who tried to send the message and which virus the message contained.

Within the messaging system, you can enable virus scanning for all users or limit it to a group of users. Limiting virus scanning to specific users is most applicable to ISP environments where users can subscribe to this service.

NOTE: Virus scanning is enabled at the Parent or User objects.

IMPORTANT: You must install one of these vendors' products before you can use NetMail's AntiVirus Agent.

Creating the AntiVirus Agent

Description: AntiVirus Agent icon

To create the AntiVirus Agent, select the messaging server on which you want to create the AntiVirus Agent; then choose AntiVirus Agent from the Create menu.

In creating the AntiVirus Agent, you are prompted for the following information:

Option	Function
Store to be monitored	The Store to be monitored is the message queue serviced by the AntiVirus Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AntiVirus Agent can monitor multiple message queues. However, you can only select one monitored queue when creating the AntiVirus agent. You can add multiple monitored queues when configuring the agent.

After you create the AntiVirus Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the AntiVirus Agent

From the AntiVirus Agent's Details menu, you can configure the following options:

IMPORTANT: You must restart AVIRUS to effect any changes in the AntiVirus Agent's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Didn't check this against interface.

Table 3 Configuring the AntiVirus Agent

Option		Function
AntiVirus Engine		
	CA InoculateIT	The AntiVirus Agent supports any Computer Associates InoculateIT-compliant virus engine. If properly configured, the NetMail AntiVirus Agent accesses the bare engine and performs all required scanning. Consequently, unless you also use the server for file and print services, Novell recommends that you do not run the full scanning engine. This allows the AntiVirus Agent to perform all required scanning to improve system performance because the agent does not scan the temporary and permanent files written by NetMail. If you need to run the full scanning product, you must first load InoculateIT in the AUTOEXEC.NCF file before loading NetMail; InoculateIT cannot start if its engine (AVENGINE.NLM) is already loaded. In this configuration, you must also ensure that you never unload InoculateIT without first unloading the NetMail AntiVirus Agent.
	McAfee	The AntiVirus Agent supports any McAfee NetShield-compliant virus engine. If properly configured, the NetMail AntiVirus Agent accesses the bare engine and performs all required scanning. Consequently, unless you also use the server for file and print services, Novell recommends that you do not run the full scanning engine. Allowing the AntiVirus Agent to perform all required scanning improves system performance because the agent does not scan the temporary and permanent files written by NetMail.

Option		Function
	Pattern-file path:	The path to the virus engine's pattern file. **IMPORTANT:** Do not include the filename. The pattern file is a virus definition file that you download periodically from the McAfee of Computer Associates web site to keep your virus protection up to date.
	Symantec CarrierScan Server	The AntiVirus Agent supports any Symantec CarrierScan-compliant engine. The Symantec CarrierScan server is the server running the virus engine.
	Host	The hostname or IP address of the server running the Symantec CarrierScan engine.
	Port	The port at which the AntiVirus Agent can connect to the CarrierScan engine.
	Command AntiVirus	
	Scanning	The scanning options determine which messages are scanned for viruses.
	Only scan messages for local recipients	Only scans messages addressed to users for whom virus scanning is enabled. You can enable virus scanning at the Parent or User objects.
	Scan all messages	Scans all messages that pass through the AntiVirus Agent's monitored queues.
	Behavior	
	Notify intended recipient if infected	Sends a virus alert to the message recipient(s). The alert indicates who tried to send the message and which virus the message contained.
	Return to sender if infected	Returns the message to the sender with a notice indicating which virus the message contained.
Monitored Queues		A monitored queue is the message queue serviced by the AntiVirus Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AntiVirus Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. To verify that an AntiVirus Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the AntiVirus Agent is listed as an NMAP client.

Option	Function
Status	By default, the AntiVirus Agent is enabled. To disable the AntiVirus Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the AntiVirus Agent at startup. However, to immediately disable the agent, you must manually unload AVIRUS.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the AntiVirus Agent is disabled, the messaging server does not launch AVIRUS.NLM again until you deselect the Disable Agent option and restart the messaging server. **NOTE:** When you initially unload AVIRUS.NLM, the messaging system is not left unprotected. Due to the design of the message queue, NMAP temporarily pauses message processing while it tries to connect to the AntiVirus Agent. It attempts a connection several times before it continues message processing without the agent. This timeout period (approximately 30 seconds) provides enough time to reload the AntiVirus Agent after updating pattern files or engine code. If you are using the InoculateIT engine without running the full scanning product, you only need to update the pattern file and/or the engine NLM. NetMail automatically detects any such update, pauses the queue, reloads the engine and the new pattern files, and then resumes message processing.

Managing User Privacy

Because the Internet is a public forum, it is important that you protect your users' personal information. The Privacy option manages what the Address Book Agent reveals about your users.

Administrators can manage users' privacy within the User object's NetMail Configuration page. Users can self-manage their privacy level from the WebAccess Options or Webmail Preferences page.

NetMail's Privacy options are executed as follows:

NOTE: Changes to these properties are implemented immediately.

Privacy Option	Function
None	The current user's e-mail address, first name, last name, and full name are returned in address book queries.
Limited	Only the current user's e-mail address is returned in address book queries.
Unlisted	The current user's personal information is not available.

Connection Manager

Description: Connection Manager icon

Connection Manager's primary function is to keep track of authenticated users. When a user logs in via POP3 or IMAP, the POP or IMAP Agent grabs the client's IP address and sends it to the Connection Manager. Connection Manager then keeps track of the IP address for a designated amount of time (the default is 15 minutes).

In NetMail 3.5, Connection Manager is utilized by the SMTP agent for SMTP-after-POP. For more information, see "SMTP-after-POP" on page 232.

IMPORTANT: For the Connection Manager to have a comprehensive record of all authenticated users, you can have only one Connection Manager per messaging system.

Creating the Connection Manager

To create the Connection Manager, select the messaging server on which you want to create the Connection Manager and choose Connection Manager from the Create menu.

After you create the Connection Manager, you must restart the messaging server. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the Connection Manager

From the Connection Manager's Details menu, you can configure the following options:

IMPORTANT: You must restart GKEEPER to effect any changes in the Connection Manager's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Table 3 Configuring the Connection Manager

Option		Function
Configuration		
	Expire Addresses after _____ minutes	The amount of time (in minutes) that an IP address is stored by the Connection Manager Agent. You can designate any value between 5 and 1440 minutes.
Status		By default, the Connection Manager Agent is enabled. To disable the Connection Manager Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Connection Manager Agent at startup. However, to immediately disable the agent, you must manually unload GKEEPER.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Connection Manager Agent is disabled, the messaging server does not launch GKEEPER.NLM again until you deselect the Disable Agent option and restart the messaging server.

Configuring the Connection Manager Settings in the Messaging Server Object

For the SMTP Agent to find the Connection Manager for SMTP-after-POP, you must configure the Conn. Mgr option in the messaging server's Identification page.

To configure this option, mark Conn. Mgr. and specify the IP address or fully distinguished name of the server running the Connection Manager.

IMPORTANT: For Connection Manager to have a comprehensive record of all authenticated users, you can only have one Connection Manager per messaging system.

11 Hosting and Feature Management

In ISP/ASP environments, you can use a single messaging system to host and provide messaging services for multiple Internet domains. Hosting multiple domains from a central messaging system presents several challenges not encountered in single-domain messaging systems. For example, there is the issue of message routing: how do you configure a single messaging system to deliver messages to users in several different Internet domains? Another issue is feature management: how do you provide each client with different sets of services using the same messaging system?

This section addresses these and other challenges associated with hosting environments. Section topics include

- "Supporting Multiple Internet Domains" on page 247
- "Domain Sharing" on page 251
- "Servicing ETRN Domains" on page 251
- "Managing Duplicate Names" on page 253
- "Managing User Aliases" on page 253
- "Managing Multiple Address Books" on page 258
- "Creating Separate Message Stores for Each Domain" on page 260
- "Auditing User Accounts" on page 260
- "Leveraging Parent Objects" on page 260

Supporting Multiple Internet Domains

To support multiple Internet domains on a single messaging system, the domains must resolve to your SMTP server's IP address and you must configure the messaging system to recognize the domains.

Configuring domains to resolve to your SMTP server's IP address is a DNS issue. Essentially, the domain's MX record must resolve to the SMTP server's host name and the host name must resolve to the server's IP address.

On the messaging system level, configuring NetMail to recognize multiple domains is an SMTP Agent issue. All Internet messages enter and leave the messaging system via the SMTP Agent. Because it is the "connection point" with the Internet, the SMTP Agent manages the messaging system's Internet domains. You must add all domains and host names that resolve to the SMTP server's IP address to the SMTP Agent's list of Global or Hosting Domains or its associated Parent objects' lists of Global or Hosting Domains before users can actually receive messages addressed to those domains.

When the SMTP Agent receives a message over the Internet, it looks at the domain portion of the recipient's e-mail address (everything after the @ symbol). If the addressed domain is one of the

SMTP Agent's Global or Hosting Domains, the message is placed in the message queue. If the SMTP Agent does not recognize the addressed domain, the message is relayed.

NOTE: The SMTP Agent does not relay the message if the number of recipients exceeds the Maximum number of recipients per mail option configured in the SMTP Agent's UBE Relaying page.

You might compromise the functionality of your messaging server if all domains and host names that resolve to the server's IP address are not added to the list of Global or Hosting Domains in the SMTP Agent or its associated Parent objects. Messages addressed to the overlooked domains are relayed to the domain's address, which actually resolves back to the messaging server. So, the server ends up relaying messages to itself in an endless loop that eventually results in 100% server utilization. The only instance in which the SMTP Agent does not relay messages to itself is if the domain resolves to the server's default IP address or the loopback IP address.

Each domain you add is either serviced by a Global Domain or a Hosting Domain. When adding a domain, determine the domain type to service your domain. Although you can have both Global and Hosting Domains in the SMTP Agent or Parent object configuration, you cannot add a single domain to both lists.

The following sections, ""Global Domains" on page 248" and ""Hosting Domains" on page 250," offer a basic explanation of the SMTP Agent's domain options and how to use them.

NOTE: For complete information on creating and configuring the SMTP Agent, see "SMTP Agent" on page 89. For more information on defining Global and Hosting domains in the Parent object, see "Configuring Parent Objects" on page 262.

Global Domains

When the SMTP Agent receives a message addressed to a Global Domain, it removes the domain portion of the e-mail address and sends the message to the queue for processing.

The basic process is as follows:

Table 3 Receiving Messages Addressed to Global Domains

Stage	Icon	Description	Recipient Address
1	 User	Someone sends a message addressed to a Global Domain.	johnd@globaldomain
2	 SMTP Agent	The SMTP Agent receives the message. It removes the domain portion of the e-mail address and transfers the message to its assigned NMAP Agent for processing in the message queue.	johnd
3	 NMAP Agent	The NMAP Agent advances the message through the queue.	johnd

Stage	Icon	Description	Recipient Address
4	 NMAP Agent	In queue 6, the NMAP Agent checks the recipient list in the control file envelope. If the recipient is within one of its assigned contexts, NMAP copies the message to the user's mailbox file. **NOTE:** For more information on user mailbox directories, see "Message Store Directory Structure" on page 19.	johnd
5	 NMAP Agent	If the user is not in its assigned context, it routes the message to the NMAP Agent that services the recipient's context.	johnd

Because Global Domains are not part of the username, you can address users serviced by Global Domains at any of the SMTP Agent Global Domains. For example, messages addressed to johnd@company.com and johnd@company.edu are delivered to the same mailbox if company.com and company.edu are both Global Domains.

Global Domain usernames require unique names. You cannot have one Global Domain user addressed as johnd@company.com and another addressed as johnd@sales.company.com.

Global Domains are most practical in corporate rather than ISP/ASP environments. First, it is more likely that usernames are unique in corporate environments than in ISP/ASP environments. Secondly, ISPs and ASPs typically host domains for unrelated organizations and the users within those organizations are associated with a specific domain. A corporation, on the other hand, can have multiple domains, but it is still a single organization. Therefore, you can address users at any of the organization's domains. Using Global Domains ensures messages are still delivered to the correct user, regardless of the addressed domain.

For the SMTP Agent to recognize Global Domains, you must include them in either the SMTP Agent's or the Parent object's Global Domains lists.

NOTE: If the Global Domain is listed under the Parent object, you must include the Parent object in the SMTP Agent's list of NetMail Parent objects.

Primary Domain

In creating the SMTP Agent, you must define the agent's Primary Domain. The Primary Domain is the Global Domain you use to identify the messaging system. By default, the SMTP Agent's Primary Domain coincides with the messaging server's Official Domain Name.

Container Domains

Use Container Domains in conjunction with Global Domains; that is, if a Container Domain is defined, include it in the Global Domains list for the SMTP Agent or Parent object.

The Address Book Agent in returning users' address book information or in determining the address book contexts a user can access can reference container Domains. (See "Address Book Agent" on page 106 for more information.)

The Modular Web Agent can also use Container Domains to generate users' Internet e-mail addresses. See "User E-mail Addresses" on page 195 for more information.

IMPORTANT: Container Domains do NOT allow you to have non-unique user IDs in different containers.

For complete information on NetMail properties for Container objects, see Table 3, “Container Objects,” on page 393.

Hosting Domains

When the SMTP Agent receives a message addressed to a Hosting Domain, it sends the message directly to the queue for processing; the entire e-mail address remains intact.

The basic process is as follows:

Table 4 Receiving Messages Addressed to Hosting Domains

Stage	Icon	Description	Recipient Address
1	 User	Someone sends a message addressed to a Hosting Domain.	annc@hosteddomain
2	 SMTP Agent	The SMTP Agent receives the message. It transfers the message to its assigned NMAP Agent for processing in the message queue.	annc@hosteddomain
3	 NMAP Agent	The NMAP Agent advances the message through the queue.	annc@hosteddomain
1	 NMAP Agent	In queue 6, the NMAP Agent checks the recipient list in the control file envelope. If the recipient is within one of its assigned contexts, NMAP copies the message to the user’s mailbox file. **NOTE:** For more information on users’ mailbox directories, see “Message Store Directory Structure” on page 19.	annc@hosteddomain
2	 NMAP Agent	If the user is not in its assigned context, it routes the message to the NMAP Agent that services the recipient’s context.	annc@hosteddomain

When the NMAP Agent is able to associate the e-mail address with a specific user, it can deliver a message. In other words, the User object’s name must match the user’s e-mail address. Therefore, users serviced by Hosting Domains must have usernames that are a combination of their name and the Hosting Domain (name@hosteddomain).

Because Hosting Domains are part of the username, you can have duplicate names in the messaging system. For example, annc@hosteddomain.com and annc@hosteddomain.org each resolve to different users. (See “Managing Duplicate Names” on page 253 for detailed information.)

Hosting Domains are most practical in ISP/ASP environments. Using Hosting Domains enables the ISP or ASP to manage duplicate names and associate users with specific domains.

For the SMTP Agent to recognize Global Domains, you must include them in either the SMTP Agent's or the Parent object's Global Domains lists.

NOTE: If the Hosting Domain is listed under the Parent object, you must include the Parent object in the SMTP Agent's list of NetMail Parent Objects.

Domain Sharing

In some environments, two separate e-mail systems can share a single domain. The Forward Local Undeliverable Messages option in the NMAP Agent enables NetMail to run alongside any application that supports Internet standards, including groupware applications such as Novell GroupWise, Lotus Notes, and Microsoft Exchange.

When the Forward Local Undeliverable Messages option is configured, the NMAP Agent forwards messages that belong to the domain but are not addressed to users within the NetMail messaging system. In the case of GroupWise, the destination server is running a GroupWise Internet Agent.

IMPORTANT: Do not "forward local undeliverable messages on both mail system; this will cause a loop if a message is sent to a user that does not exist on either system.

NOTE: For more information, see the Forward Local Undeliverable Messages property in Table 4, "Configuring the NMAP Agent," on page 68.

Servicing ETRN Domains

ETRN Domains are messaging systems that use a hosting service, such as an ISP or ASP, to send and receive messages over the Internet. These systems have their own messaging servers, agents, and mail directories; however, all their messaging services are local. Consequently, they must use a hosting service to send and receive remote messages. In most instances, ETRN Domains have non-persistent dial-up connections to their ISP or ASP.

Because these systems have their own user accounts and mailboxes, the hosting ISP or ASP cannot service them as a Global Domain or Hosting Domain. Instead, you must list it as Relayed Domains in the SMTP Agent or Parent object. As Relayed Domains, the host service simply queues the remote system's messages until the ETRN Domain establishes a connection and requests its messages using the ETRN command.

NOTE: For more information on the ETRN protocol, see RFC 1985.

Configuring NetMail at the Remote Site

When using a NetMail server at the remote site, the SMTP Agent's Mail Relay Host option must point to the IP address or host name of the hosting service's SMTP server. This enables the remote site to transfer its outbound messages to the hosting service, which then relays the messages over the Internet.

Additionally, you must select the SMTP Agent's Send ETRN option. In transferring its outbound messages, the remote site's SMTP server must send the command **`ETRN domain`** when it connects with the Mail Relay Host. The ETRN command indicates to the hosting server that the remote site is on line and to send the queued messages for this domain.

Another requirement is that one of the remote domain's MX records must resolve to its own server's hostname. This means that the server must have the same IP address every time it comes on line or that a dynamic DNS must publish the MX record.

NOTE: Because some DNS servers still cache dynamic DNS records, publishing the MX record with dynamic DNS is less reliable.

Additionally, it is required that the preference number assigned to this MX record is lower than any other MX record associated with the ETRN domain. This gives the remote server first priority in receiving messages addressed to the ETRN domain.

Configuring NetMail at the Host Site

When using a NetMail server as an ETRN host, select the SMTP Agent's Accept ETRN option. This allows the SMTP Agent to accept ETRN commands from remote servers. When the hosting server receives the **`ETRN domain`** command from a remote server, it issues a command to its NMAP agent to send all messages queued for the remote domain.

If the SMTP Agent's UBE Relaying features are configured, you must add ETRN Domains to the Relayed Domains (ETRN) list in the SMTP Agent or Parent object. Then, the SMTP agent can relay messages for those domains.

The ETRN domain must also have an MX record that resolves to the hosting server's hostname. It is required that the preference number assigned to this MX record is higher than the preference number assigned to the MX record associated with the remote host. This ensures the ETRN domain's messages are only routed to the host server if the remote server is unavailable.

Using Message Forwarding as an Alternative to ETRN

Many hosting services do not provide ETRN services because it requires a static IP address. However, with the introduction of Parent objects in NetMail 3.5, these organizations can now use Message Forwarding to provide a similar service.

To configure this option, follow these steps:

1. Create a Parent object for the remote domain.
2. List the remote domain as either a Global or Hosting Domain in the Parent object.

   NOTE: If you add the remote domain as a Hosting Domain, you can use the Task-Oriented Management feature to delegate user account administration to the remote site. See "Task-Oriented Management" on page 262 for more information.
3. Create User objects for all users at the remote site and associate them with the Parent object.
4. Create a User object for the remote site. This dummy account serves as the remote site's general mailbox.
5. Configure the Parent object's Forwarding option to forward all messages to the dummy account. Do not mark Keep Local Copy.

   This forwards every message addressed to users associated with the Parent object to the dummy account without replicating the messages in the individual users' mailboxes.
6. Install a POP utility at the remote site that pulls messages from the dummy mailbox and redistributes them in the local messaging system.

For more information on the Parent object's Forwarding option, see the Forwarding property in Table 3, "Configuring Parent Objects," on page 262.

Managing Duplicate Names

Another challenge associated with hosting multiple domains in a single messaging system is managing duplicate names. NetMail requires that all usernames in the tree are unique, regardless of the user's Container object. Consequently, no two users in any domain can have identical usernames.

NetMail easily addresses this issue with the use of Hosting Domains. Rather than coming up with different variations of every user's name, administrators can simply use the full Internet e-mail address (name@domain).

References NetWare Administrator. Needs updated.

To create User objects that include the user's name and domain, NetWare Administrator requires that the period in the domain name be "escaped." For example, the user jling@hostdomain.com is created and displayed in NetWare Administrator as jling@hostdomain\.com.

Employing users' e-mail addresses as their usernames means that they must type their full username (name@domain) to log in to the messaging system.

NOTE: Do not use this option with NetWare 4.*x* because it does not support usernames with periods.

To prevent the SMTP Agent from stripping out the domain portion of the username before it delivers the message to the queue, the administrator must list each domain as a Hosting Domain in the SMTP Agent or Parent object configuration menu. (For information on configuring the SMTP Agent, see "SMTP Agent" on page 89. For information on configuring Parent objects, see "Configuring Parent Objects" on page 262.)

NOTE: In POP mode, Netscape Messenger 4.x strips @ symbols and trailing characters from usernames. In Hosting Domains, users can use Netscape Messenger 4.x in IMAP mode or they can manually configure the POP client

To enable the Netscape Messenger 4.*x* POP client to accept usernames with the @ symbol, edit the PREFS.JS file in the C:\PROGRAM FILES\NETSCAPE\USERS*USERNAME* directory. Add the following line above the other mail lines:

```
user_pref("mail.allow_at_sign_in_user_name", true)
```

You can then restart the Netscape Messenger 4.*x* POP client. You can make this change before distributing the Netscape client to all the users.

Managing User Aliases

A standard service ISPs provide to their clients is user aliasing. Aliases are usernames that resolve to another account. For example, a common alias present on most web sites is "webmaster." In most cases, webmaster is not the account owner. Instead, webmaster@company.com most likely resolves to another user's mailbox like johnsmith@company.com.

The NetMail Alias Agent allows administrators to define e-mail aliases, either automatically or manually. The automatic aliasing feature pulls information directly from eDirectory™ to generate aliases for User objects. For instance, a user named Steve Johnston could receive messages addressed to Steve_Johnston, Steve.Johnston, SJohnsto, and so on.

Manually defined aliases can correspond to any Internet e-mail address, perhaps based on function, such as our earlier example of webmaster@company.com. These aliases resolve to the user who is assigned with that function.

The aliases configured in the Alias Agent are not defined as Alias objects in eDirectory. They are maintained by the Alias Agent and are specific to your NetMail messaging system.

Existing Alias objects are automatically recognized by NetMail. Because these aliases are defined in eDirectory, they function independently of the Alias Agent. Messages addressed to Alias objects are automatically delivered to the associated user's mailbox—no Alias Agent is needed.

IMPORTANT: NetMail Aliasing does not work if Verify Recipient Addresses When Accepting Messages is selected in the SMTP Agent configuration. When this option is enabled, the SMTP Agent intercepts messages before they are processed in the message queue; consequently, messages addressed to NetMail aliases are deleted before the Alias Agent can process them. For more information, see the Verify Recipient Addresses When Accepting Messages property in Table 4, "Configuring the SMTP Agent," on page 91.

Creating an Alias Agent

To create an Alias Agent, select the messaging server on which you want to create the agent; then choose Alias Agent from the Create menu.

In creating the Alias Agent object, you are prompted for the following information:

Option	Function
Monitored Queues	Monitored Queues are the NMAP Agent contexts for which the Alias Agent can automatically generate aliases. When the Alias Agent generates automatic aliases, it references the Monitored Queues list. If a username exists within the selected NMAP Agents' contexts, the Alias Agent creates an alias. If the username does not exist within a supported context, no alias is created. When creating the Alias Agent, you can only select one Monitored Queue. You can add multiple Monitored Queues when configuring the agent.

After you create the Alias Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the Alias Agent

From the Alias Agent's Details menu, you can configure the following options:

IMPORTANT: You must restart MSGALIAS to effect any changes in the Alias Agent's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Table 5 Configuring the Alias Agent

Option		Function
Configuration		
	Scheduler	
	Automatically Create Database Every _____ Day(s)	How often (in days) the Alias Agent regenerates the alias database. The default is 1 day. The maximum setting is 99 days. The alias database contains alias tables that store the aliases and their associated usernames. **NOTE:** 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 SNMP is configured).

Option		Function
	Aliasing	
	Automatic Creation of Aliases from User Objects	Automatically generates aliases for User objects in the following formats: ◆ Firstname_Lastname@Domain (Steve_Johnston@novell.com) ◆ First Letter+Lastnam@Domain (Sjohnsto@novell.com) This alias option is limited to eight characters. ◆ Firstname.Lastname@Domain(Steve.Johnston@novell.com) ◆ Full.M.Name@Domain (Steve.W.Johnston@novell.com) ◆ Full_M_Name@Domain (Steve_W_Johnston@novell.com) The Fullname formats only work if the users' full names are typed in the Full Name field of their User objects. Automatically generated aliases are local aliases. Consequently, they are only recognized by the current Alias Agent. To ensure that these aliases are recognized throughout the messaging system, you can have only one Alias Agent.
Local Aliases		Aliases that are only recognized by the current Alias Agent. They are stored in the local Alias Agent's alias table. Local aliases are ideal when you are maintaining identical aliases, such as Admin or Webmaster, in a single messaging system. (See "Configuring Multiple User Objects Simultaneously" on page 208 for more information.) The following are the most common errors encountered with local aliases: ◆ The replacement string does not correspond to a valid username. ◆ The alias resolves to more than one user. ◆ The replacement string does not exactly match the username. ◆ The alias is not an exact match. ◆ If the user belongs to a Hosting Domain, the replacement string must match the user's full e-mail address (username@hostdomain). ◆ If the user does not belong to a Hosting Domain, the replacement string does *not* include the domain portion of the user's e-mail address.

Option		Function
	Add	To create a local alias in NetWare Administrator, 1. Type an alias in the left field. 2. Type the corresponding e-mail address (replacement string) in the right field. If the replacement string addresses a user in a Global Domain, type only the username. You cannot type the complete e-mail address because the domain portion of Global Domain e-mail addresses is stripped out by the SMTP Agent before the message enters the queue. For more information, see "Global Domains" on page 248. 3. Click Add. The alias appears in the list using the following syntax: *alias* string = *user_name* For example, if user SJohnsto wants users to send e-mail to SteveJ, the alias reads: SteveJ = SJohnsto. Then when users address e-mail to SteveJ, it is delivered to the SJohnsto mailbox. You could also create an alias such as feedback@company.com that would resolve to a local or remote e-mail address. 4. When you are finished providing aliases, click OK to save the aliases to the Alias Agent's local alias table.
	Remove	To remove an alias, select the alias > click Remove.
	Import	**IMPORTANT:** The Import option is only available in NetWare Administrator. You can import local aliases in ASCII format if they use an *alias string*= *user_name* syntax with a carriage return and line feed (<CR><LF>) between lines. To import local aliases, 1. Click Import. 2. Browse to and select the ASCII file of aliases. 3. Click OK.
	Global Aliases	Aliases that are recognized by every Alias Agent running on a distributed messaging server. Global aliases are stored in a shared alias table in the Internet Services container. The shared alias table includes entries from every Alias Agent running on a distributed messaging server. Other than the fact that global aliases are recognized throughout the messaging 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. **NOTE:** The preferred way to manage Global Aliases is to define Alias objects. This is because Alias objects provide all the functionality of Global Aliases, but they do not require an Alias Agent. (You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create Alias objects.)

Option		Function
	Add	See Local Aliases.
	Remove	See Local Aliases.
	Import	See Local Aliases.
	Queue Server	Queue Servers are the message queues monitored by the Alias Agent. Messages passing through the specified NMAP Agents' message queues are scanned by the Alias Agent. If a message recipient matches any of the Alias Agent's defined aliases, it replaces the alias with the corresponding e-mail address. A single Alias Agent can monitor multiple NMAP Agents' message queues. Use the Browse button to locate and select one or more NMAP Agents. **NOTE:** You cannot configure multiple Alias Agents to monitor the same NMAP Agent. Only one Alias Agent can monitor each NMAP server. To verify that an Alias Agent is registered to a particular NMAP Agent, view the Client property in the NMAP object. If registered, the server running the Alias Agent is listed as an NMAP client.
	Monitored Queues	Monitored Queues are the NMAP Agent contexts for which the Alias Agent can automatically generate aliases. Use the Browse button to locate and select one or more NMAP Agents. When the Alias Agent generates automatic aliases, it references the Monitored Queues list. If a username exists within the selected NMAP Agents' contexts, the Alias Agent creates an alias. If the username does not exist within a supported context, no alias is created. To verify that an Alias Agent is registered to a particular NMAP Agent, view the Client property in the NMAP object. If registered, the server running the Alias Agent is listed as an NMAP client.
	Status	By default, the Alias Agent is enabled. To disable the Alias Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Alias Agent at startup. However, to immediately disable the agent, you must manually unload MSGALIAS.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Alias Agent is disabled, the messaging server does not launch MSGALIAS.NLM again until you deselect the Disable Agent option and restart the messaging server.
	Internet E-mail Address Automatic Attribute Population	

Option		Function
	Automatically populate “Internet E-mail Address” attribute	Automatically populates the User object attribute, Internet E-mail Address, with one of the following values: ◆ Default E-mail address For information on how the default e-mail address is derived, see “User E-mail Addresses” on page 195. ◆ Firstname_Lastname@Domain (Steve_Johnston@novell.com) ◆ First Letter+Lastnam@Domain (Sjohnsto@novell.com) This alias option is limited to eight characters. ◆ Firstname.Lastname@Domain(Steve.Johnston@novell.com) ◆ Full.M.Name@Domain (Steve.W.Johnston@novell.com) ◆ Full_M_Name@Domain (Steve_W_Johnston@novell.com) **NOTE:** The Fullname formats only work if the users' full names are provided in the Full Name field of their User objects.

Alias Agent Contexts

You can only generate automatic aliases for those users that belong to the messaging system. For standalone messaging servers, this means the user must belong to a local NMAP context. For distributed messaging servers, this means that the user must belong to an NMAP context for one of the messaging servers in Internet Services. If the username does not exist within the local messaging server’s NMAP context list, you cannot generate automatic aliases for that user. However, you can manually create aliases for users inside or outside the local messaging system.

NOTE: For more information on how NMAP contexts are managed, see the Context property in Table 4, “Configuring the NMAP Agent,” on page 68.

Managing Multiple Address Books

Domain-specific address books are a fairly standard client request. In messaging systems that support a single organization, it is very easy to provide a system-wide address book. However, in messaging systems that support multiple organizations, providing domain-specific address books can become very complicated.

NetMail 3.5 simplifies the process. The following steps outline the procedure for providing domain-specific address books in a multi-domain messaging system. To facilitate the explanation, we use abc.com is our sample domain.

1. Create a Parent object for abc.com.
2. List abc.com as either a Global or Hosting Domain in the Parent object. For our example, abc.com is a Hosting Domain.

   NOTE: By adding abc.com as a Hosting Domain, you can use the Task-Oriented Management feature to delegate user account administration to someone at abc.com. See “Task-Oriented Management” on page 262 for more information.
3. Associate all users in abc.com with the abc Parent object.
4. Create a User object for abc.com. This dummy account serves as the domain’s address book account. In this case, the account is addressbook@abc.com and the password is abc1.

5 Create the Address Book Agent. (See "Creating the Address Book Agent" on page 107 for further information.)

NOTE: You can actually implement this configuration using any LDAP server.

6 Using a DS editing tool such as NDS Snoop, reset the value of the Novonyx:LDAP Options attribute to include the following options:

Option	Value
LDAP_REQUIRE_BASEDN	4
LDAP_REQUIRE_AUTHENTICATION	8
LDAP_USE_USERS_BASEDN	16

NOTE: For further information on resetting the value of the Novonyx:LDAP Options attribute, see "Address Book Agent Optional Features" on page 110.

These options enable the Require Authentication, Derive Search Domain from Authentication, and Require Search Domain features. The Require Authentication feature requires a username and password when users connect to the Address Book Agent.

The Derive Search Domain from Authentication feature configures the Address Book Agent to derive the user's search domain from the username given during authentication. For details on this process, see the LDAP_USE_USERS_BASEDN properties in Table 3, "NovonyxLDAP Options, Value, and Description," on page 111.

The Require Search Domain feature requires that a search domain is included in the address book configuration. Specify the Search Domain in the LDAP server URL or in the address book client.

7 From the Parent object's ModWeb Mail page, mark System-Wide and use the following LDAP parameters in the LDAP URL:

ldap://*user*:*password*@*hostname*:*port*/?*basedn*

- The *user*:*password* variable is the user's name and password.
- *Hostname* identifies the LDAP server's host name or IP address.
- *Port* specifies the LDAP port assignment. If the LDAP server uses the default LDAP port (port 389), you do not need to specify a port.
- *Basedn* identifies the address book context. This is required if the Require DN option is added to the Address Book Agent. It is ignored if the Derive DN from Authentication attribute is added to the Address Book Agent.

With the Require Authentication and Derive DN from Authentication added to the Address Book Agent, and using the default LDAP port, the LDAP URL for abc.com's System-Wide address book would be

ldap://addressbook@abc.com/?ldap.abc.com

Using the dummy account's username and password automatically authenticates users with the Address Book Agent and, because Derive DN from Authentication is marked, it ensures that all users associated with the abc.com Parent object can only view other abc.com users in the Modular Web client's System-Wide address book.

NOTE: You can also manage multiple address books with POP and IMAP clients; however, you must configure the LDAP information, such as username, password, and basedn in the individual clients.

Creating Separate Message Stores for Each Domain

The original location of the message store is defined when creating the NMAP Agent. This is the default message store for all users in the NMAP Agent's assigned contexts.

NOTE: For a complete discussion of the structure and contents of the message store, see "Message Store Directory Structure" on page 19. For more information on the NMAP Agent's message store property, see the Message Store property in Table 4, "Configuring the NMAP Agent," on page 68.

Locating all the users' mailboxes in a single message store works well within single organizations; however, when hosting domains for multiple organizations, using a single message store makes it difficult to identify which mailboxes belong to each domain. Creating different message store directories for each domain allows you to easily identify and manage resources for a specific domain.

You can define domain-specific message stores using Container objects.

When NetMail is installed, Container objects take on NetMail properties. The Container object's NetMail Options property includes an option to define a custom message store for users within the current container.

The Container object message store is the volume and directory where the mailboxes for users in the current container are located. It does not affect the general message queue and SCMS directories, which are always located in the default message store volume and directory.

To define a domain-specific message store using Container objects, you would put all the domain's User objects in a single container and then define a Container object message store.

For complete information on NetMail Container object properties, see Table 3, "Container Objects," on page 393.

Auditing User Accounts

Many ISPs and ASPs charge their clients for the number of user accounts they host on their servers and for the services they provide for those users. IMSAudit is a NetWare® utility that can assist these organizations in auditing their clients' accounts.

IMSAUDIT allows ISPs and ASPs to determine the total number of active NetMail mailboxes on their messaging system and the specific features that are enabled for each user. Disabled users or users who have never logged in are not counted.

In NetMail 3.5, IMSAudit runs an audit report on the entire tree. On all operating systems, the IMSAUDIT.LOG file is saved in the \DBF directory configured in the Messaging Server object.

NOTE: For more information, see "IMSAUDIT" on page 330.

Leveraging Parent Objects

Two of the most effective ways to leverage the Parent objects in multi-domain environments is to manage agent services and to distribute system management. The following sections, "Feature Management" on page 261 and "Task-Oriented Management" on page 262, explore these options in detail.

Feature Management

Many ISPs and ASPs have a fee-per-service arrangement with their clients; that is, they charge their clients based on the level of services they provide. Consequently, it is important that these organizations are able to provide different services for each Internet domain without having to dedicate a separate messaging server for each set of client services.

NetMail enables administrators to manage agent services for individual users or groups of users. This means that administrators can run an agent on the messaging server, but enable, disable, or selectively define that agent's services for each of their clients. This is accomplished by configuring the agent options in the client's Parent object or individual User objects. An explanation of each option is provided in the following section.

Parent Object Feature Management

The Parent object's primary function is to manage agent services in multi-domain environments. In defining Parent objects, administrators can enable, disable, or configure options for the following agent services:

- IMAP
- POP
- Forward
- Autoreply
- Messaging Rules
- NMAP
- Task Oriented Management
- ModWeb Mail
- ModWeb Preferences
- Modular Web Agent
- SMTP
- Mail Proxy
- Calendar Agent
- Calendar and Scheduling
- AntiVirus

To incorporate the Parent object settings, administrators must associate the Parent with specific User objects by selecting the Parent in the User object's NetMail Parent Object page. Administrators can apply this setting en masse using utilities such as Bulkloader or ICE.

For detailed information on the Parent object's configuration options, see "Configuring Parent Objects" on page 262.

User Object Feature Management

The User object replicates most of the configuration options available in Parent objects. This duplication lets the administrator configure general settings in the Parent object, but create "exceptions to the rule" in individual User objects. For example, in the Parent object the administrator can set a mailbox quota for users in an Internet domain. However, at the User object level, the administrator can allocate a larger mailbox quota for the domain's webmaster.

For a complete explanation of each option in the User object Details menu, see Table 5, "User Objects," on page 394.

Task-Oriented Management

Using Parent objects, you can off-load the task of maintaining user accounts allow you to the individuals who actually manage employee information. For a complete description of this functionality, "Task-Oriented Management" on page 262

Creating Parent Objects

To create the Parent object, select the Parent Objects container (or the container in which you want to create the Parent object) and choose Parent from the Create menu. In creating the Parent object, you are prompted to type the Parent object name.

Configuring Parent Objects

From the Parent object's Details menu, you can configure the following options:

Table 3 Configuring Parent Objects

Option			Function
Features			
	Options		Changes to these properties are implemented immediately.
		Object Description	Text provided in this field is displayed in the TOM administrator interface. You can use this field to provide information or instructions for the TOM administrator.
		Default Inheritance	Determines precedence. If there are conflicting configurations between the Parent and User objects, you can specify which object you want to take precedence.
		Parent First	Parent object settings take precedence over the User object settings. If the Parent setting is not configured, the User setting is used.
		User First	User object settings take precedence over the Parent object settings. If the User setting is not configured, the Parent setting is used.
	Features		
		IMAP	Changes to this property are implemented immediately.
		IMAP Access	Allows the administrator to enable or disable IMAP connections for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
		POP	Changes to this property are implemented immediately.
		POP Access	Allows the administrator to enable or disable POP connections for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
Internet Mail			
	Forwarding		Changes to this property are implemented immediately.

Option		Function
	Forward Ability	Allows the administrator to enable or disable messaging forwarding for users associated with the current Parent object. If Enabled is selected, the Parent object's Forwarding settings are in effect for all users associated with the Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
	Forwarding	
	Forward Mail To	The e-mail address to which incoming messages are forwarded. Mark the Forward Mail To option to forward all messages received by users associated with the current Parent object to the designated e-mail address. Use this option to provide relaying services for remote messaging systems. For details, see "Using Message Forwarding as an Alternative to ETRN" on page 252.
	Keep Local Copy	Keeps a copy of all forwarded messages in the users' mailboxes. If Keep Local Copy is not marked, incoming messages are simply forwarded; they are not delivered to the users' mailboxes.
Auto Reply		Changes to this property are implemented immediately.
	AutoReply Ability	Allows the administrator to enable or disable autoreply messaging for users associated with the current Parent object. If Enabled is selected, the Parent object's AutoReply/Vacation settings are in effect for all users associated with the Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
	AutoReply/ Vacation	
	Reply to all received mail with message	Sends the defined autoreply message in response to all messages received by users associated with the current Parent object. The autoreply message is only sent to the original sender; not all message recipients.
Messaging Rules		Changes to this property are implemented immediately.
	Rule Usage Ability	Allows the administrator to enable or disable the Rules feature for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
NMAP		Changes to this property are implemented immediately.
	Mailbox Quota	
	Use parent quota, fallback to user quota	Uses the mailbox quota configured in the Parent object. If no mailbox quota is configured in the Parent object, the setting defers to the mailbox quota defined in the User object.
	Disabled	Disables all mailbox quotas for users associated with the current Parent object. This includes mailbox quotas configured in the Parent object, User object, or NMAP Agent.

Option		Function
	Use user quota, fallback to parent quota	Uses the mailbox quota configured in the User object. If no mailbox quota is configured in the User object, the setting defers to the mailbox quota defined in the Parent object.
	Per-user mailbox quotas	The mailbox quota applied to all users associated with the current Parent object. Type the maximum mailbox size in the kByte field. Messages, folders, and calendar items count against the mailbox quota.
Task Oriented Management		
(Task Oriented Management		Allows the administrator to give selected users rights to create, import, modify, or delete user accounts in the contexts and domains designated in the current Parent object. For more information, see “Task-Oriented Management” on page 262. **NOTE:** The rights to create, import, modify, or delete user accounts are granted in the User object under the Task-Oriented Management property. (See Table 5, “User Objects,” on page 394 for more information.) These properties only apply to TOM administrators associated with the current Parent object. All changes to Task-Oriented Management properties are immediately implemented. **NOTE:** All task-oriented management functions are enabled by the Modular Web Agent Task Management Module. Although the module itself has no configurable options, to provide TOM functionality via WebAccess, it must run on the messaging server.
	Managed domain names	The Hosting Domains which TOM administrators can select when creating new user accounts. The usernames for new Hosting Domain accounts include the selected domain’s name (name@hosted_domain). See “Hosting Domains” on page 250 for information on Hosting Domain usernames. If this field is left blank, the domain defaults to the messaging system’s Official Domain as defined in the messaging server configuration. Therefore, the default Internet e-mail address for new Global Domain accounts is username@official_domain. However, due to the nature of how Global Domains are handled in NetMail, you can actually address these users at any of the messaging system’s Global Domains. See “Global Domains” on page 248 for more information on how Global Domain addressing works. If you type any domain in this field, NetMail assumes it is a Hosting Domain and all new users are created with a corresponding username (name@hosted_domain). **IMPORTANT:** The TOM module verifies that the listed domains are valid Hosting Domains. To ensure a valid Hosting Domain, you must include the domain in either the SMTP Agent’s or the Parent object’s Hosting Domains lists. If the Hosting Domain is listed under the Parent object, you must include the Parent object in the SMTP Agent’s list of NetMail Parent Objects. If the TOM administrator selects multiple Hosting domains when creating the user, the User object is created with the first domain name and Alias objects are created with the subsequent domain names. For example, if the TOM administrator selects domains abc.com and 123.com when creating a user account for jotero, the User object is created as jotero@abc.com. The Alias object, jotero@123.com, points to jotero@abc.com.

Option		Function
	Managed contexts	The NMAP context(s) in which TOM administrators can create, modify, delete, or import user accounts. If multiple contexts are selected, NetMail equally distributes User objects among the contexts.
	Maximum number of allowed users	The number of users that any TOM administrator can create associated with the current Parent object.
ModWeb Mail		Changes to this property are implemented immediately.
Limits		
	Maximum number of recipients per mail	The maximum number of recipients for messages sent by users associated with the current Parent object.
	Message Size LImit	The maximum size of messages that users can send associated with the current Parent object.
Address Book		
	Personal Addressbook	Enables users associated with the current Parent object to create personal address books. Users' personal address books are stored in their User object. Consequently, users can access their personal address book from any location as long as they are logged in to the network.
	System-Wide LDAP Server	If marked, this option gives users associated with the current Parent object access to a system-wide address book in the Modular Web client (WebAccess or Webmail). In the LDAP URL field, you can provide the following LDAP parameters: ldap://user:password@hostname:port/?basedn ◆ The *user:password* variable is the user's name and password. ◆ *Hostname* identifies the LDAP server's host name or IP address. If you type the IP address of a server running the Address Book Agent, users can access address book information from eDirectory. ◆ *Port* specifies the LDAP port assignment. If the LDAP server uses the default LDAP port (port 389), you do not need to specify a port. ◆ *Basedn* identifies the address book context. This is required if the Require DN attribute is added to the Address Book Agent. It is ignored if the Derive DN from Authentication is added to the Address Book Agent. (See "Address Book Agent Optional Features" on page 110 for more information.) Users with the Privacy attribute set to Limited or None in their User object are visible to other NetMail users in the System-Wide Address Book. Users with an Unlisted privacy setting are not visible in the System-Wide Address Book. **NOTE:** For information on providing domain-specific address books, see the Context property in Table 3, "Information Needed When Creating an NMAP Agent Object," on page 68.

Option		Function
	Public LDAP Server	If marked, this option allows users associated with the current Parent object to define their own public address book in the Modular Web client (WebAccess or Webmail). To define a default Public LDAP Server, type the host name or IP address of any public LDAP server in the LDAP URL field. You can use the same LDAP parameters discussed under System-Wide LDAP Server. **NOTE:** Users can designate a different Public address book in the Modular Web client interface.
ModWeb Preferences Module		Changes to this property are implemented immediately.
	Password Settings	
	Allow user to change password	Enables users associated with the current Parent object to change their eDirectory password in the Modular Web client (Webmail or WebAccess). Because NetMail is completely integrated with eDirectory, the only password it recognizes is the user's eDirectory password. Therefore, marking this option actually gives users rights to change their eDirectory password, regardless of whether they have rights to the actual password property in their User object.
	SSL Required	Requires an SSL connection between the Modular Web client and the messaging server before users associated with the current Parent object can change their passwords.
	Disable Options	Disables user configuration options in the WebAccess and Webmail templates. If marked, these options do NOT appear in the User Preferences menu.
	Timeout	The amount of idle time before the user is automatically logged out of the Modular Web client. Template color definition options. This option is specific to the Webmail template.
	Privacy	The user's level of privacy within the messaging system. The privacy level controls what the Address Book Agent reveals about the user.
	Signature	Custom text automatically inserted at the end of each message.
Modular Web Agent		Changes to this property are implemented immediately.
	Configuration	
	Identifier	Users that are associated with the current Parent object see this banner in the title bar of each WebAccess page.
	Default Language	The default language for the Modular Web Agent and its sub-modules. This setting is implemented for users associated with the current Parent object.
	Default Timezone	The default time zone for the Modular Web Agent and its sub-modules. This setting is implemented for users associated with the current Parent object.

Option		Function
	Modular Web Access	Allows the administrator to enable or disable the Modular Web client for users associated with the current Parent object. If Enabled is selected, the Parent object's Modular Web Agent settings are in effect for all users associated with the Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
Template		NetMail WebAccess templates allow you to control the Modular Web Agent client interface. NetMail 3.5 ships with two client templates—WebAccess (Webacc.ctp) and Webmail (WebMail.ctp). The WebAccess interface provides standard mail client functionality, calendaring, scheduling, assigning tasks, and writing notes. Administrators can also use the WebAccess interface to delegate NetMail administrative functions such as adding, modifying, and deleting user accounts. (For more information on delegating NetMail administration, see "Task-Oriented Management" on page 262.) Webmail is patterned after the NIMS 2.5 mail client interface. It provides standard mail client functionality and administrators can use the Webmail interface to give users access to self-administration features like changing passwords and configuring vacation messages. For more information on templates, see "Calendar Agent" on page 99.
	Default Template	The default mail client template for users associated with the current Parent object. Select the default template from the Available Templates list. **NOTE:** Users can select a different template in the mail client interface.
	Available Templates	The templates that users associated with the current Parent object can select in the Modular Web client. To add templates to the list, 1. Click the Browse button (...). 2. Click Add to browse the tree for Template objects. **NOTE:** To add a template to the list of available templates, you must first create a Template object in the Template container.
SMTP		Changes to this property are effective within 5 minutes.
	Global Domains	The Global Domains associated with the current Parent object. You can associate Parent objects with both Global and Hosting Domains. **IMPORTANT:** Do not list a domain as both a Global Domain and a Hosting Domain. For the SMTP Agent to recognize Global Domains, you must include them in either the SMTP Agent's or the Parent object's Global Domains lists. For a complete discussion on how the messaging system uses Global Domains, see "Global Domains" on page 248. For an explanation of the SMTP Agent's configuration options, see "Configuring the SMTP Agent" on page 90.

Option		Function
	Hosting Domains	The Hosting Domains associated with the current Parent object.You can associate Parent objects with both Hosted and Global Domains. **IMPORTANT:** Do not list a domain as both a Global Domain and a Hosting Domain. For the SMTP Agent to recognize Global Domains, you must include them in either the SMTP Agent's or the Parent object's Global Domains lists. For a complete discussion on how the messaging system uses Hosting Domains, see “Hosting Domains” on page 250. For an explanation of the SMTP Agent’s configuration options, see “Configuring the SMTP Agent” on page 90.
	Relayed Domains (ETRN)	The current SMTP Agent services the ETRN Domains. To support these domains, you must click the Accept ETRN option in the Options page. For more information on ETRN Domains, see “Servicing ETRN Domains” on page 251.
	Allowed Hosts	A list of IP ranges. Select the Require sender to be in “Allowed” list for remote sending option in the SMTP Agent to limit the workstations that fall within the designated IP address ranges that can relay messages through the SMTP server. This prevents users who are not members of the messaging system from using the SMTP Agent to relay messages over the Internet. Use this setting to prevent internal hosts from relaying Internet messages. To restrict which workstations that you allow to send remote messages, designate ranges of internal IP addresses. **NOTE:** If a workstation’s IP address is not in an Allowed Hosts range, you can still use the workstation to send local messages (i.e., messages to other users in the messaging system).
Calendar Agent		Changes to this property are immediately implemented.
	Calendar Access	Allows the administrator to enable or disable iCal functionality, including automatic event status tracking, for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
	Mail Proxy	Changes to this property are immediately implemented.
	Mail Proxy Access	Enables or disables the user’s ability to proxy other e-mail accounts. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the calendar and scheduling options are enabled.
Calendar/Scheduling		Changes to this property are implemented immediately.
	Calendar Access	Enables or disables the user’s Calendar(s) and scheduling functions. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the calendar and scheduling options are enabled.
AntiVirus		Changes to this property are implemented immediately.
	Virus scanning	Allows the administrator to enable or disable virus scanning options for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.

12 Managing Mailing Lists

NetMail List Agent allows administrators to create and maintain mailing lists. Mailing lists are essentially public communication forums. Use mailing list to broadcast information via e-mail. Mailing list members can be assigned to a particular mailing list, such as a company newsletter roster, or they can subscribe to a mailing list, such as a news publication.

This section provides the information you need to configure and manage mailing lists.

The topics covered in this chapter include

- "List Agent" on page 269
- "NDS Mailing Lists" on page 271
- "Mailing Lists" on page 273
- "List User Objects" on page 277
- "eDirectory Groups" on page 278
- "List Server Administration" on page 279
- "List Server Commands" on page 279

List Agent

Description: List Agent icon

Before you can use mailing lists, you must create and configure the List Agent. The List Agent provides list server and NDS mailing list functionality in your NetMail system.

The List Agent references the Mailing Lists container for names and members of mailing lists when scanning the message queue for messages addressed to mailing lists. Consequently, every NDS Mailing List and Mailing List object must be represented in the Mailing Lists container for the List Agent to find it. If an NDS Mailing List or Mailing List is created elsewhere in the tree, it must have an Alias object in the Mailing Lists container.

NOTE: You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Mailing Lists container.

IMPORTANT: Because the List Agent references the Mailing Lists container for all mailing list information, it is recommended that you partition the Internet Services container and replicate it on the list server.

Creating a List Agent Object

To create the List Agent, select the messaging server on which you want to create the List Agent and choose List Agent from the Create menu.

In creating the List Agent, you are prompted for the following information:

Option	Function
Store to be monitored	The Store to be monitored is the message queue serviced by the List Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single List Agent can monitor multiple message queues. However, you can only select one monitored queue when creating the List agent. You can add multiple monitored queues when configuring the agent.

After you create the List Agent, you must restart the messaging server to load the agent. For information on restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Configuring the List Agent

From the List Agent's Details menu, you can configure the following options:

IMPORTANT: You must restart IMSLIST to effect any changes in the List Agent configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Table 3 Configuring the List Agent

Option	Function
Schedule	
Configuration	
Create Digests Daily At _____ hours	The time each day when the List Agent compiles and distributes Mailing List digests. Specify the time using the 24-hour clock. A digest is a compilation of the messages broadcast over a mailing list in a 24-hour period. The List Agent only generates digests for Mailing List objects that have the Generate Digest option selected in the mailing list configuration menu.
Monitored Queues	A monitored queue is the message queue the List Agent monitors for messages addressed to mailing lists. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single List Agent can monitor multiple message queues. Use the Browse button to select one or more monitored queues. **NOTE:** You cannot configure multiple List Agents to monitor the same queue. Only one List Agent can monitor each queue. To verify that a List Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the List Agent is listed as an NMAP client.

Option	Function
Status	By default, the List Agent is enabled. To disable the List Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the List Agent at startup. However, to immediately disable the agent, you must manually unload IMSLIST.NLM or restart the messaging server. For information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the List Agent is disabled, the messaging server does not launch IMSLIST.NLM again until you deselect the Disable Agent option and restart the messaging server.

NDS Mailing Lists

Description: NDS Mailing List icon

NDS mailing lists allow you to broadcast messages to User objects in eDirectory™. NDS mailing lists can be comprised of User objects, Groups, Aliases, Organizational Roles, or Container objects.

NOTE: If a Container object is selected, messages are forwarded to the users within the designated Container object.

Users receive messages for each instance they are represented in the Mailing List. For example, if a user is represented in both a User object and a Container object, the user receives two messages every time a message is posted to the mailing list.

Unlike regular mailing lists, users cannot subscribe to NDS mailing lists; rather, they are assigned by their administrator.

Since a mailing list is like a communication forum, the list administrator does not receive status messages if one of the members' addresses is no longer valid or if a particular message failed.

Because the List Agent references the Mailing Lists container for all mailing list information, NDS Mailing List objects are typically created in the Mailing Lists container. However, you can create an NDS Mailing List elsewhere in the tree if you also create an Alias object for it in the Mailing Lists container.

NOTE: You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Mailing Lists container.

Creating an NDS Mailing List

To create an NDS Mailing List object, select the Mailing Lists container (or the container in which you wish to create the object) and choose NDS List from the Create menu.

In creating the Mailing List object, you are prompted for the following information:

Option	Function
Name of List	A unique name for the Mailing List object. List names cannot duplicate usernames or group names within eDirectory.
Owning NMAP Store	The NMAP message store that contains the mailing list mailbox. The mailbox contains the mailing list's digest and archive files. (Use only if you select archive or digest options.) Use the Browse button to select the NMAP Agent you want to manage the mailing list's mailbox.

Configuring an NDS Mailing List

This entire table needs revised to match the updated interface.

From the Mailing List's Details menu, you can configure the following options:

NOTE: Changes to the NDS Mailing List configuration are implemented immediately.

Table 3 Configuring an NDS Mailing List

Option		Function
Configuration		
General		
	Abstract	A description of the mailing list that is included in the welcome message sent to users.
	Description	A detailed description of the mailing list. The mailing list description is returned when a user sends a **`review list_name detailed`** command to the List server. See "User Commands" on page 280 for a complete list of commands.
	Senders	One or more users who are authorized to send to this NDS mailing list. Senders must belong to the local messaging system. Click the Browse button to select one or more senders in the Directory tree.
	Members	The eDirectory objects belonging to the mailing list. You can include on NDS Mailing Lists: User objects, Groups, Aliases, Organizational Roles, or Container objects.
Options		
	Require Sender to Authenticate via SMTP	Mark this option to require users to authenticate with the messaging system before sending to the mailing list. Users can authenticate through SMTP or send the message through the Modular Web Agent client. Requiring SMTP authentication ensures that anyone sending a message to the NDS mailing list is who they say they are. This prevents unauthorized users from sending to the list.

Option	Function
NMAP Store	The NMAP message store that contains the mailing list mailbox. The mailbox contains the mailing list's digest and archive files. (Use only if you select archive or digest options.) Use the Browse button to select the NMAP Agent you want to manage the mailing list's mailbox.

Mailing Lists

Description: Mailing List icon

A list server mailing list is a compilation of user e-mail addresses. When a message is sent to the mailing list, the message is automatically forwarded to the mailing list members.

Typically, users subscribe to list server mailing lists. To subscribe to a list server mailing list, users send a message to the mailing list's e-mail address with the word "subscribe" in the body of the message.

Since a mailing list is like a communication forum, the list administrator does not receive status messages indicating if one of the members' addresses is no longer valid or if a particular message failed.

Because the List Agent references the Mailing Lists container for all mailing list information, Mailing List objects are typically created in the Mailing Lists container. However, you can create an Mailing List elsewhere in the tree if you also create an Alias object for it in the Mailing Lists container.

NOTE: You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Mailing Lists container.

Creating a Mailing List

To create a Mailing List object, select the Mailing Lists container (or the container in which you wish to create the object); then select Mailing List from the Create dialog.

In creating the Mailing List object, you are prompted for the following information:

Table 4 Creating a Mailing List

Option	Function
Name of List	A unique name for the Mailing List object. List names cannot duplicate usernames or group names within eDirectory. By default, Mailing List objects are associated with the messaging system's gLobal Domains; that is, the list can be addressed at any Global Domain properly configured in a Parent object or the SMTP Agent. For example, if a given messaging system has three Global Domains, a user can subscribe to mailing list ABC at any of the following addresses: ABC@globaldomain1, ABC@globaldomain2, or ABC@globaldomain3. To associate a mailing list with a Hosting Domain, the list name must include the Hosting Domain name (*list_name@hosted_domain*). In this case, the list can only be addressed at the designated domain.
Owning NMAP Store	The NMAP message store that contains the mailing list mailbox. The mailbox contains the mailing list's digest and archive files. (Use only if you select archive or digest options.) Use the Browse button to select the NMAP Agent you want to manage the mailing list's mailbox.

Configuring a Mailing List

From the Mailing List's Details menu, you can configure the following options:

NOTE: Changes in the List Server Mailing List configuration are implemented immediately.

Table 5 Configuring a Mailing List

Option		Function
Configuration		
General		
	Abstract	A description of the mailing list that is included in the welcome message sent to users when they subscribe to the list.
	Description	A detailed description of the mailing list. The mailing list description is returned when a user sends a **`review list_name detailed`** command to the List server. See "User Commands" on page 280 for a complete list of commands.

Option		Function
	Moderators	The List User(s) assigned to moderate the mailing list. (See “List User Objects” on page 277.) Click the Browse button to select a List User object from the current Mailing List. Moderators can perform the following mailing list functions: ◆ Manage and change List User attributes by sending commands through their mail client. ◆ Add and delete users from the mailing list in bulk ◆ Receive messages to be moderated. (See the moderated property in Table 5, “Configuring a Mailing List,” on page 274 for information on moderated lists.) If multiple moderators are selected, all moderators can manage and change List User attributes or add users to and delete users from the mailing list. However, only the first moderator in the list receives messages to be moderated. **NOTE:** Moderators CANNOT create lists.
	Subscriptions	
	Open	Anyone can subscribe to the mailing list.
	Closed	Only the NetMail administrator can add members to the mailing list.. **NOTE:** Mailing List moderators cannot add members to a closed list.
	Review	
	Public	List members can query information about the list. (See “User Commands” on page 280 for a complete list of query commands.)
	Private	Only the list moderator can query information about the list. (See “User Commands” on page 280 for a complete list of query commands.)
	Owner	List information is not accessible via e-mail; you can use WebAdmin to query information about the list.

Option		Function
	Postings	
	Moderated	All messages addressed to the mailing list are first sent to the moderator. The moderator can make changes before posting the message to the mailing list. To post the message, the moderator simply forwards the message to the list. Rather than moderating all messages sent to the mailing list, you can choose to only moderate messages from specific users by selecting Postings require approval in the List User configuration. (See "List User Objects" on page 277 for more information.)
	By Moderator only	Only the moderator can send messages to the mailing list.
	Non-members may post	Anyone can send messages to the mailing list.
	Point Reply-To to List:	Sends reply messages to everyone in the mailing list. If this option is not marked, reply messages are only sent to the original sender.
	Block Attachments	Blocks attachments on mailing list messages. Messages with attachments are bounced.
	Options	
	Plaintext Signature	Appends the plain text signature defined on the Signatures page to every plaintext message sent to the mailing list.
	HTML Signature	Appends the HTML signature defined on the Signatures page to every HTML message sent to the mailing list.
	Keep Archive	Archives all messages sent to the mailing list. Archived messages are kept in an archive folder in the mailing list's mailbox. (See the NMAP Store property in Table 5, "Configuring a Mailing List," on page 274 for information on the mailing list mailbox.) For practicality and convenience, you can search archived messages. Messages are not put in the archive folder until after the digest is created. If the Generate Digest option is not selected, messages are sent directly to the archive folder.
	Generate Digest	Generates a digest of all messages sent to the current Mailing List object. This option allows users to subscribe to a mailing list digest instead of receiving mailing list messages individually. Mailing list digests are compilations of the messages broadcast through a mailing list in a 24-hour period. Digests have a table of contents in the body of the message and mailing list messages are included as attachments. The List Agent generates and distributes digests on a daily basis. (See the Create Digests Daily at ____ hours property in Table 3, "Configuring the List Agent," on page 270 for more information.)
Signatures		
	Plaintext	The signature that is automatically appended to plain text messages.
	HTML	The signature that is automatically appended to HTML messages. The signature can include HTML formatting codes.

Option	Function
NMAP Store	The NMAP message store that contains the mailing list mailbox. The mailbox contains the mailing list's digest and archive files. (Use this only if you select archive or digest options.) Use the Browse button to select the NMAP Agent you want to manage the mailing list's mailbox.

List User Objects

Description: List User Objects icon

List User objects represent the members of a list server mailing list. When users subscribe to a mailing list, a List User is added to the respective Mailing List object. Administrators can also add mailing list members by creating List User objects within the Mailing List object.

Creating List User Objects

To create a List User object, select the Mailing List to which you wish to add the user and select List User from the Create dialog.

In creating a List User object, you are prompted for the following information:

Option	Function
E-mail address of list users	The subscribing user's complete e-mail address.

Configuring List User Objects

From the List User's Details menu, you can configure the following options:

NOTE: Changes to the List User configuration are implemented immediately.

Table 6 Configuring List User Object

Option			Function
Options			
	General		
		Full name	The user's full name.
		Options	
		Receive list messages	The current user receives all messages sent to the list. This property is the equivalent of the **`Set list_name Mail | NoMail`** command.

Option		Function
	Receive list digests	The current user receives a digest of messages sent to the list. This property is the equivalent of the **`Set list_name Digests | NoDigests`** command. Mailing list digests are compilations of the messages broadcast through a mailing list in a 24-hour period. Digests have a table of contents in the body of the message and mailing list messages are included as attachments. The List Agent generates and distributes digests on a daily basis.
	Send copy of own postings	Copies the user on all his or her postings to the mailing list. This property is the equivalent of the **`Set list_name Repro | NoRepro`** command.
	Don't show user	Hides the user's full name and e-mail address. When someone requests the list's member information using the **`Review list_name Detailed`** or **`Lists Detailed`** commands, the current user's information does not appear. This property is the equivalent of the **`Set list_name Conceal | NoConceal`** command.
	Banned user	The current user cannot post to the mailing list. This property is the equivalent of the **`Set list_name Ban | NoBan`** command.
	Postings require approval	The current user's postings must be approved by a mailing list moderator. (For more information, see the Moderators property in Table 5, "Configuring a Mailing List," on page 274.) This property is the equivalent of the **`Set list_name Verify | NoVerify`** command.

eDirectory Groups

Description: eDirectory Groups icon

Do not confuse eDirectory groups with NDS Mailing Lists or List Server Mailing Lists. While you can use groups as mailing lists—messages addressed to eDirectory groups are broadcast to group members and messages are addressed to mailing lists—they do not provide the features specific to mailing lists. For example, administrators cannot control who can send messages to groups.

Another difference between groups and mailing lists is status information. Users sending messages to groups receive status information if one of the group member addresses is no longer valid or if the message fails. This is not true for mailing lists. A mailing list is considered a communication forum; consequently, users do not receive message status information

Finally, because groups are independent eDirectory objects, sending messages to eDirectory groups does not require a list server. However, every member of the group must be represented by

a User object. This means you can only use eDirectory Groups to send messages to users within your messaging system.

List Server Administration

Administrators manage all List objects using WebAdmin. From WebAdmin, administrators can create new Mailing Lists or NDS Mailing Lists, add users to a mailing list, and set List User options.

List Server Commands

Moderator Commands

Moderators cannot perform any administrator functions such as creating new Mailing Lists or NDS Mailing Lists. However, they can add users to a Mailing List and set List User options by e-mailing commands to the list server (listserv*@your.domain*). Commands must be located in the message body, *not* the subject line.

The following table outlines the commands the moderator can use to manage Mailing List accounts.

NOTE: The minimum acceptable abbreviation is listed in capital letters. Square brackets indicate optional parameters.

Table 7 List Server Moderator Commands

Command	Description
ADD *list_name e-mail_address* [*fullname*] PW=*password*	Enables the list moderator to add list users.
DELETE *list_name e-mail_address* [*fullname*] PW=*password*	Enables the list moderator to delete list users.
PW *list_name* [Add | Change] *new_password* [PW=*old_password*]	Sets or changes the moderator's List User object password. The moderator's password is required each time he or she performs a secured administrative function such as adding members to or deleting members from the mailing list. **NOTE:** This property is hidden and does not appear in the List User configuration menu. (See "Configuring List User Objects" on page 277.)
SET *list_name*	The moderator can use the SET command with the following parameters to configure List User properties. (see "Configuring List User Objects" on page 277).
BAN | NOBan FOR *e-mail_address* PW=*password*	The designated user cannot receive messages from or post messages to the mailing list. The difference between banning a user and simply deleting a user is that a deleted user can resubscribe. Banning prevents a user from resubscribing or having any access to the mailing list.

Command	Description
VERify | NOVerify FOR *e-mail_address* PW=*password*	The designated user's postings must be approved by a mailing list moderator.
CONceal | NOConceal FOR *e-mail_address* PW=*password*	Hide/show the designated user's full name and e-mail address. When someone requests the list's member information using the **`Review <list_name> Detailed`** or **`Lists Detailed`** commands, the designated user's information does not appear.
MAIL | NOMail FOR *e-mail_address* PW=*password*	The designated user receives all messages sent to the list.
DIGests | NODigests FOR *e-mail_address* PW=*password*	The designated user receives a daily digest of messages sent to the list. Mailing list digests are compilations of the messages broadcast through a mailing list in a 24-hour period. Digests have a table of contents in the body of the message and mailing list messages are included as attachments.
REPro | NoRepro FOR *e-mail_address* PW=*password*	The designated user receives a copy of all his or her postings to the mailing list.
ACK | NOAck FOR *e-mail_address* PW=*password*	The designated user receives notification from the list server when his or her messages are posted to the mailing list.

User Commands

Users can subscribe to the list server, select list server services, or unsubscribe from the list server by e-mailing the following commands to the list server (listserv*@your.domain*). Commands must be located in the message body, *not* the subject line.

NOTE: The minimum acceptable abbreviation is listed in capital letters.

Table 8 List Server User Commands

Command	Description
SUBscribe *list_name*	Subscribe to a list. If the list is under a hosting domain, the <*list_name*> must include the hosting domain name (i.e. SUBscribe <*list_name*>@<*hosted_domain*>).
SIGnoff *list_name* UNSubscribe *list_name*	Unsubscribe from a list.
SIGnoff *UNSubscribe *	Unsubscribe from all lists.
SET *list_name*	Use the SET command with the following parameters to configure List User properties. (see "Configuring List User Objects" on page 277.) *The designated parameters are applied to the message sender*.

Command	Description
CONceal | NOConceal	Hide/show your full name and e-mail address. When someone requests the list's member information using the **`Review <list_name> Detailed`** or **`Lists Detailed`** commands, the current user's information does not appear.
MAIL | NOMail	Receive all messages sent to the list.
DIGests | NODigests	Receive a daily digest of messages sent to the list. Mailing list digests are compilations of the messages broadcast through a mailing list in a 24-hour period. Digests have a table of contents in the body of the message; mailing list messages are included as attachments.
REPro | NRRepro	Receive a copy of all your postings to the mailing list.
ACK | NOAck	Receive a notification from the list server when your messages are posted to the mailing list.
QUEry *list_name*	Receive a listing of your personal settings (such as digests | nodigests; conceal | noconceal, etc.) for the designated mailing list.
QUEry *	Receive a listing of your personal settings for all mailing lists on the current List server.
INFo	Receive a comprehensive listing of all list server commands.
HELp	Receive a listing of the most commonly used list server commands.
RELease	Receive information about the List Agent host and the List Agent's software version.
THAnks	Receive a verification that the list server is alive.
REView *list_name*	Receive a listing of the mailing list's configuration settings. (See "Configuring a Mailing List" on page 274.)
REView *list_name* Detailed	Receive a listing of the mailing list's configuration settings and its member information. (See "Configuring a Mailing List" on page 274.) **NOTE:** If a List User is concealed (SET *<list_name>* CONCeal), his or her e-mail address and full name are not included in the membership list.
LISts	Receive a listing of all the list server's mailing lists.
LISts Detailed	Receive a listing of all the list server's mailing lists and their members. **NOTE:** If a List User is concealed (SET *list_name* CONCeal), his or her e-mail address and full name are not included in the membership list.
INDex *list_name*	Receive an index of the mailing list's available archive files. This is only valid if the mailing list is configured to archive.
GET *list_name message_ID*	Receive a specific message from the list's archive. The archived message is included as an attachment in the return message. This command is only valid if the mailing list is configured to archive.

Command	Description
SEArch *list_name*	The SEArch command enables users to search archived messages by date, subject line, or message body. The following parameters can be combined using AND/OR statements. For example, to search for a message sent between January 1, 2001 and January 31, 2001 and containing “Performance Review” in the subject line, the user would submit the following command: SEArch *list_name* FROM 01/01/2001 TO 31/01/2001 AND SUBJECT “Performance Review”
FROM *dd/mm/yyyy* TO *dd/mm/yyyy*	Receive a listing of all archived messages posted to the mailing list between the specified dates.
FROM *dd/mm/yyyy* TO today	Receive a listing of all archived messages posted to the mailing list from the date indicated to today.
SUBJECT “*subject*”	Receive a listing of all archived messages that include the indicated text string in the subject line. The quotes are required to demarcate the text string. Quotes cannot be searched or escaped.
SENDER “*sender*”	Receive a listing of all archived messages posted to the mailing list by the designated sender. The quotes are required to demarcate the sender. Quotes cannot be searched or escaped.
BODY “*body_text*”	Receive a listing of all archived messages that include the indicated text string in the message body. The quotes are required to demarcate the text string. Quotes cannot be searched or escaped.

A Sample NetMail Configurations

This appendix provides practical examples of the following standard NetMail configurations:

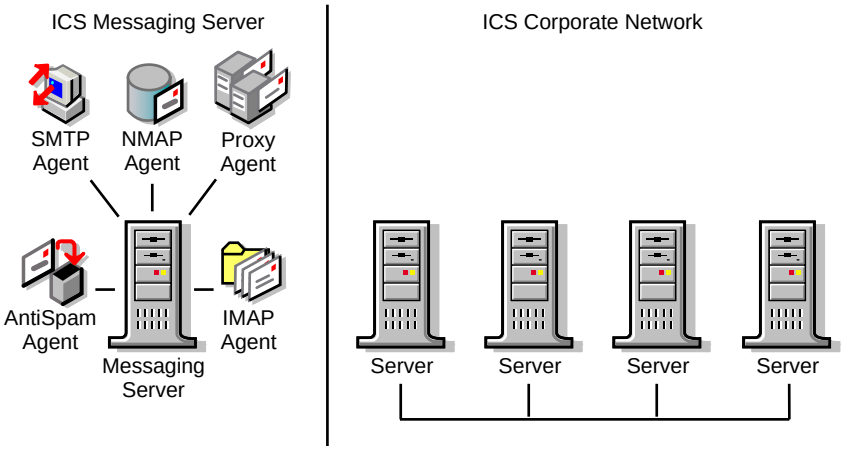
- "Single Server Network" on page 283
- "Single Messaging Server LAN" on page 284
- "Multiple Standalone Messaging Server LAN" on page 285
- "Multiple Distributed Messaging Server LAN" on page 286
- "Multiple Messaging Server WAN" on page 288

For a detailed explanation of these configurations, see Chapter 2, "Planning Your NetMail System," on page 27.

Single Server Network

ICS is an ASP that provides e-mail 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 WebAccess, 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.

Description: ICS (ASP) Messaging Server and Agents in a Single Server 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.

Hardware

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.

Messaging System Configuration

The messaging server and its associated agents are located in the Internet Services container.

For users to access agent services (IMAP, SMTP, and Proxy), individually assign every container with User objects belonging to the messaging system as an NMAP context.

NOTE: Individually assign NMAP contexts because they are not inherited.

eDirectory Configuration

Because the entire Directory tree resides on a single machine, the messaging server automatically has local access to the messaging server object and all user objects in the tree. Therefore, no additional eDirectory™ configuration is necessary.

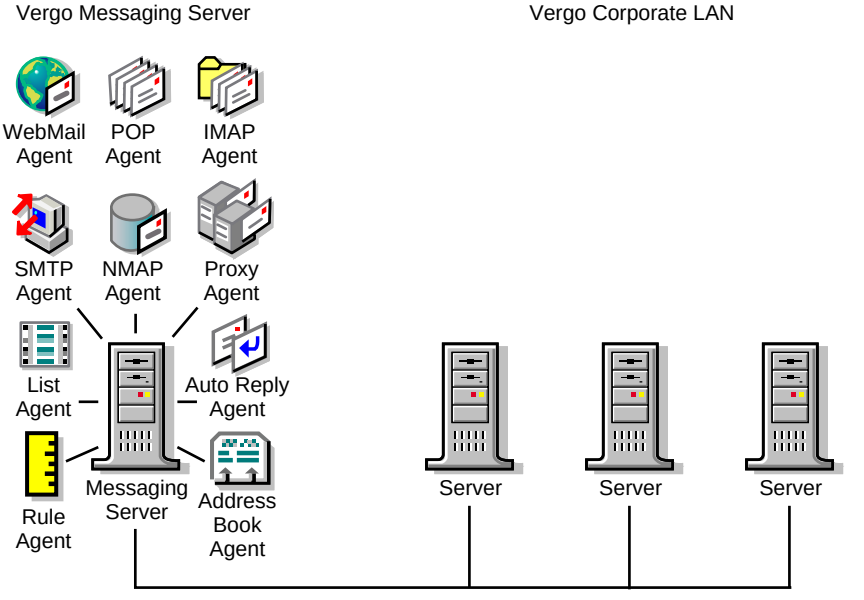
Single Messaging Server LAN

Vergo Enterprises currently has a single LAN with three servers and 1500 workstations. Messaging services include WebAccess, POP, IMAP, Address Book, SMTP, AutoReply, Proxy, List and Rules.

Hardware

You can manage a messaging system of this size with one additional dedicated messaging server with a Pentium II 300 MHz processor, 512 MB of RAM, and 10 GB in disk space.

Description: Vergo Enterprises Messaging Server and Agents configuration



Messaging System Configuration

The messaging server and its associated agents are located in the Internet Services container.

For users to access agent services, individually assign every container with User objects belonging to the messaging system as an NMAP context.

NOTE: Individually assign NMAP contexts because they are not inherited.

eDirectory Configuration

Given that the current network has three servers, the fourth server (the messaging server) does not automatically have local access to the messaging server object or the messaging system's user objects.

To give the messaging server local access to the Messaging Server object and all User objects in the messaging system, you must do the following:

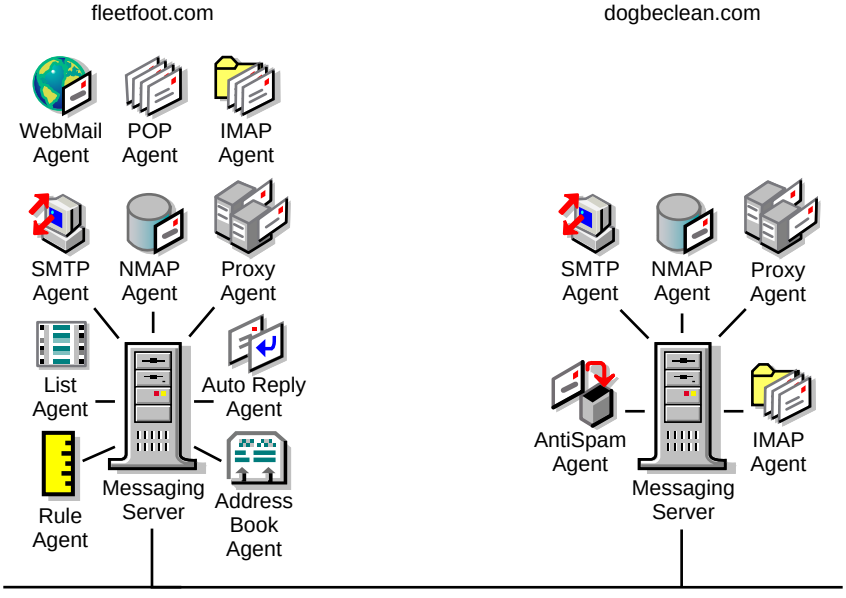
- Partition the Internet Services container.
- Partition the NMAP Agent's user contexts.
- Create a read/write replica of the Internet Services and user context partitions on the messaging server.

Multiple Standalone Messaging Server LAN

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 standalone messaging servers. For example, two of StormFront's largest customers, FleetFoot and DogBeClean, each have standalone messaging servers.

Description: FleetFoot and DogBeClean Messaging Servers and Agents configurations



Messaging System Configuration

In configuring this multiple standalone message server LAN, you need to do the following:

- Install NetMail on each messaging server. Only extend the eDirectory schema during the first installation. On subsequent installations, only include the Novell® NetMail files.
- Create each messaging server object in the container associated with its users (i.e. fleetfoot or dogbeclean).
- Enter the client's domain name (i.e. fleetfoot.com and dogbeclean.com) in the messaging server's Official Domain Name field.
- Mark Disable Distributed Processing in each messaging server's configuration menu to create a standalone messaging server.
- Create and configure NetMail agents.

  Because standalone messaging servers function independently of each other, they must have all the NetMail agents required for a self-contained messaging system.

  At a very minimum, each messaging server must have NMAP, SMTP, and a client agent (POP, IMAP, or the Modular Web Agents). Additional agents depend on the customer's needs.

  NOTE: The NMAP, SMTP, POP, IMAP, Modular Web Agent, AutoReply, Rule, Proxy, Alias, AntiSpam, AntiVirus, List, and Connection Manager must run locally on standalone messaging servers.
- Assign NMAP contexts. For users to access agent services (IMAP, SMTP, and Proxy), individually assign every container with User objects belonging to the dogbeclean messaging system as an NMAP context on the dogbeclean messaging server. Likewise, assign all user contexts belonging to the fleetfoot messaging system as NMAP contexts on the fleetfoot messaging server.

  NOTE: Individually assign NMAP contexts because they are not inherited.

eDirectory Configuration

Because multiple servers exist on the network, each messaging server does not automatically have local access to its associated Messaging Server and User objects.

To give each standalone messaging server local access to its Messaging Server and User objects, you must do the following:

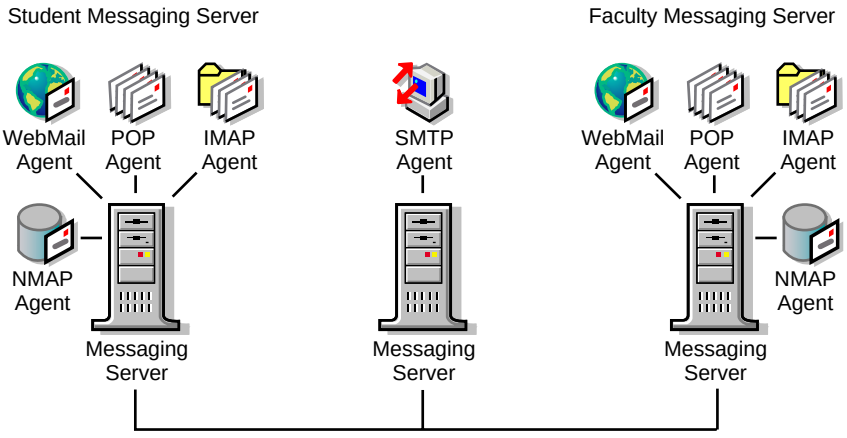
- Partition the fleetfoot and dogbeclean containers.
- Create a read/write replica of the fleetfoot and dogbeclean partitions on their associated messaging servers.

Multiple Distributed Messaging Server LAN

The Royal Academy is a major university research center with approximately 25,000 students and faculty. The university offers a broad range of programs in the fields of medicine and science.

The university's LAN has 10,000 users with approximately 95 servers. The university's IT department wants to manage faculty and students on separate messaging servers and they want a dedicated mail relay host for a single point of contact with the Internet.

Description: Royal Academy Multiple Distributed Messaging Server LAN configuration



Messaging System Configuration

In configuring this multiple distributed messaging server LAN, you need to do the following:

- Install NetMail on each messaging server. Only extend the eDirectory schema during the first installation. On subsequent installations, only include the Novell NetMail files.
- To easily delegate system administration, create the student and faculty Messaging Server objects in the same containers as the users they service and simply grant administrative rights on a container basis.
- Create the messaging server for the dedicated mail relay host in the Internet Services container.
- To enable the student and faculty messaging servers to locate and interact with one another and the mail relay host, create an Alias object for the student and faculty messaging servers in the Internet Services container.

  NOTE: You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Internet Services container.
- Create and configure NetMail agents.
  - To completely separate students and faculty, give the student and faculty messaging servers their own NMAP and mail client agents.
  - The dedicated mail relay host runs the SMTP Agent.
- Assign NMAP contexts. For users to access agent services (IMAP, SMTP, and Proxy), individually assign every container with User objects belonging to the student messaging system as an NMAP context on the student messaging server. Likewise, assign all user contexts belonging to the faculty messaging system as NMAP contexts on the faculty messaging server.

  NOTE: Individually assign NMAP contexts because they are not inherited.
- Configure the NMAP Agent's Trusted Hosts.
  - To prevent the mail relay host from having to authenticate with the student and faculty servers, make the SMTP server a trusted host of the student and faculty servers' NMAP Agents.
  - To prevent the student and faculty servers from having to authenticate with one another, make the student and faculty servers trusted hosts of one another's NMAP Agent.

eDirectory Configuration

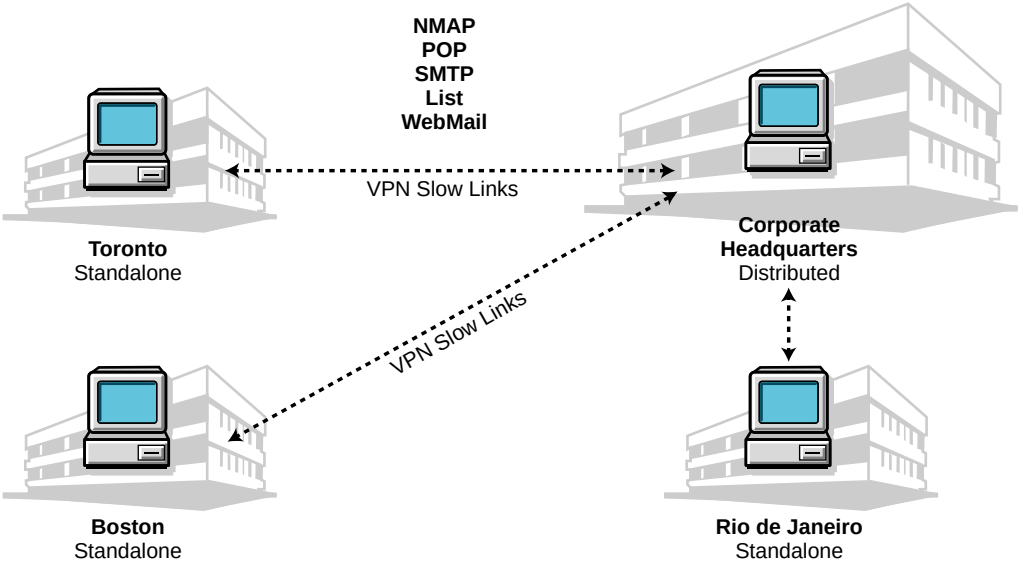
Because there are 95 servers in the network, the messaging servers do not automatically have local access to their Messaging Server and User objects. To give each messaging server local access to its associated objects, you must do the following:

- Partition the Internet Services container.
- Partition the student and faculty containers.
- Create a read/write replica of the Internet Services partition on the SMTP server.
- Create a read/write replica of the student and faculty partitions on their associated messaging servers.

Multiple Messaging Server WAN

Reesis, Inc. is an international pharmaceutical company. Reesis' headquarters are in Princeton, New Jersey and research labs are located in Boston, Toronto, and Rio de Janeiro.

Description: Reesis Multiple Messaging Server WAN configuration



Messaging System Configuration

- Install NetMail on a messaging server in each office. Only extend the eDirectory schema during the first installation. On subsequent installations, only include the Novell NetMail files.
- Create Princeton's Messaging Server object in the Internet Services container. This is the messaging system's only distributed messaging server.
- Create the Boston, Toronto, and Rio Messaging Server objects in the same containers as the users they service.
- Mark Disable Distributed Processing in the messaging server configuration menu to create standalone messaging servers in Boston, Toronto, and Rio. Creating standalone messaging servers in the remote offices minimizes network traffic across the WAN and still provides fast, efficient service to remote users.

- Create and configure NetMail agents.
  - Because this system has several standalone messaging servers and only one distributed messaging server, each server must run all the NetMail agents required for a self-contained messaging system.

    At a very minimum, each messaging server must have NMAP, SMTP, and a client agent (POP, IMAP, or the Modular Web Agents).
  - The one exception is the Address Book Agent. Reesis wants a corporate address book. Because the remote servers have access only to their local eDirectory 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, install the Address Book Agent on Princeton's messaging server. To access the Address Book Agent, users must configure their e-mail client to use the Princeton messaging server as an LDAP server. They can do this by entering the host name and LDAP port number of the Princeton server in their e-mail client's System or Public address book fields.

    NOTE: The Address Book Agent's default LDAP port assignment is port 389 or, on Novell Nterprise Linux Services, port 52389.
- Assign NMAP contexts. For users to access local agent services (IMAP, SMTP, and Proxy), assign each NMAP Agent to every user context belonging to its local messaging system. For example, the administrator assigns Boston's NMAP Agent all user contexts belonging to Boston's local messaging system.

  NOTE: Individually assign NMAP contexts because they are not inherited.
- To enable users in remote offices to send messages to the central messaging system and each other, configure the Boston, Toronto, and Rio NMAP Agents to forward local undeliverable messages to Princeton's distributed messaging system.
- To enable the distributed messaging server in Princeton to send or forward messages to users in Boston, Toronto, and Rio, represent the remote messaging servers by a Alias objects in the Internet Services container.

  NOTE: You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create the Alias object in the Internet Services container.
- To prevent Princeton's messaging server from having to authenticate with the remote servers, make Princeton's messaging server a trusted host of the Boston, Toronto, and Rio servers' NMAP Agents.

eDirectory Configuration

To minimize network traffic and still give each messaging server local access to its associated objects, you must do the following:

- Partition the Internet Services container.
- Partition the user contexts assigned to the Princeton messaging server.
- Partition the Boston, Toronto, and Rio containers.
- Create a read/write replica of the Internet Services and user context partitions on Princeton's messaging server.

- Create a read/write replica of the Boston, Toronto, and Rio partitions on their associated messaging servers. This reduces the number of partitions that you must replicate across the WAN to one per messaging server.

B Message Structure

This appendix reviews the structure of messages as they come into the messaging system, pass through the message queue, and are stored in the user's mailbox or SCMS directory.

Section topics include

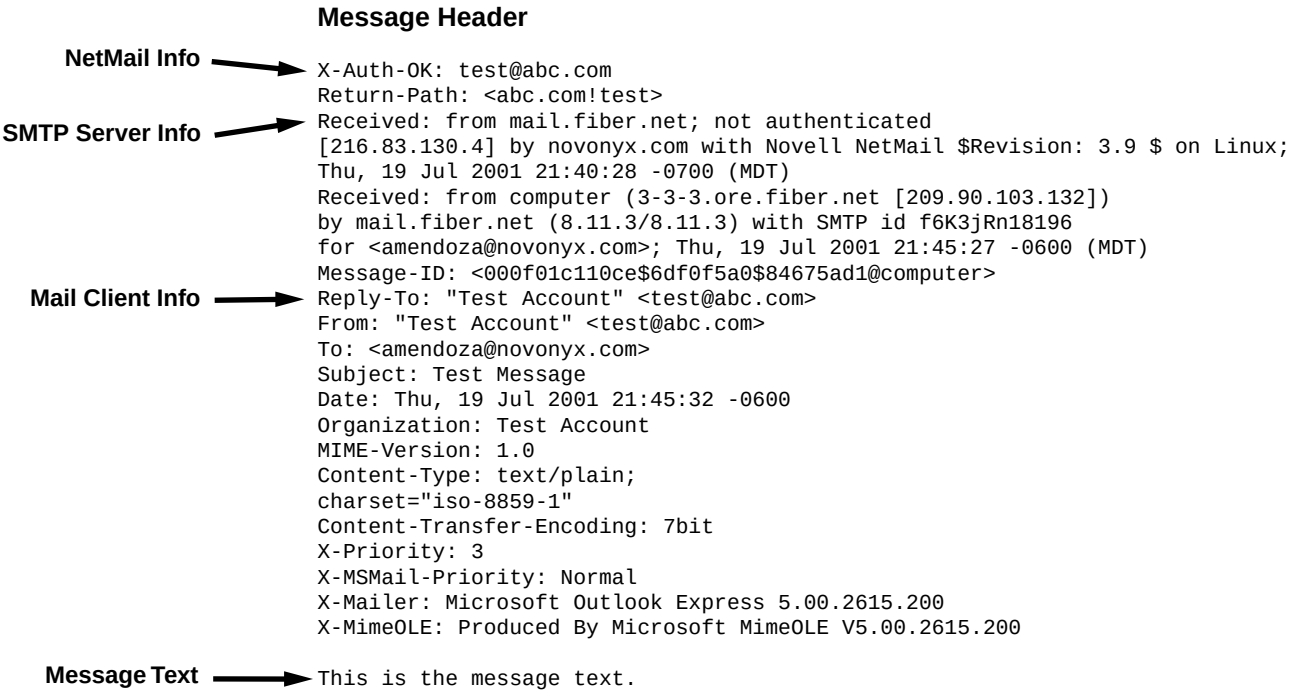
- "Message Structure" on page 291
- "Control File Structure" on page 293
- "Data File Structure" on page 293
- "SCMS Message Structure" on page 294
- "Mailbox File Structure" on page 294

For details on the accompanying directory structures, see "Message Processing" on page 19.

Message Structure

The following is a message as viewed in WebAccess or Webmail using the View Source option.

Description: Parts of Message Header using View Source option



NetMail, the SMTP server, and the mail client all put information in the message header. The NetMail information identifies the account the sender used to authenticate with NetMail. This information is only displayed if SMTP-after-POP or SMTP authentication is enabled on the sender's messaging system. If these options are not enabled or if the sender is not on a NetMail messaging system, the X-Auth value is "No."

The SMTP Server Info is generated by the SMTP server(s) that relayed the message. This information varies per server; however, in general, it identifies the IP address and host name of the server(s) that relayed the message. This information is useful in tracking SPAM. Although spammers are able to falsify their identity and part of the message path, it is difficult to falsify the last server used to relay the message.

NOTE: The message's last relay point is identified in the first line of the message's SMTP Server Info section.

The Mail Client Info section of the message is generated by the sender's mail client. Again, this information varies per mail client, but in general it contains the To, From, Date, and Subject line along with any message flags and encoding information.

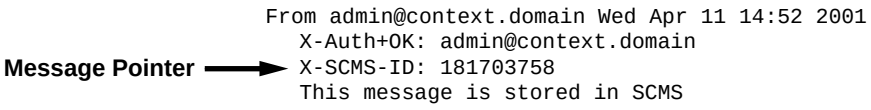
The final section of the message is the actual message text. It contains the message text and any attachments.

Control File Structure

NMAP creates the control file (C*xxxxxxx*.*) when a message enters the message queue. (See "Message Processing in the Message Queue" on page 21 for more information.) Agents, like the SMTP and Modular Web Agents, that drop messages in the message queue issue commands that cause the NMAP Agent to create the control file. The control file contains most of the information necessary to process the message.

The following is a sample control file:

Description: Sample Control File



Each line of the control file corresponds to one of the following flags:

Table 9 Control File Structure

Flag	Description
D	Date–the date the control file was created.
F	From–the message sender's e-mail address.
R	Remote Recipients–recipients not within the local messaging system. Messages entering the queue via the Modular Web client initially list all recipients as remote. Local recipients aren't identified until queue 6. Messages entering the queue via the SMTP Agent already have the local and remote recipients identified.
L	Local Recipients–recipients within the local messaging system.
M	Folder–if an active rule directs the message to a specific folder, this flag identifies the mailbox folder NMAP copies the message to.
X	An internal flag NetMail uses for processing.
C	Calendar item–identifies the recipients of the data file's calendar items (i.e., notes, appointments, or tasks).

If the message has multiple local recipients, NMAP copies the message to the recipients' mailboxes one at a time. When the message is delivered to a user's mailbox, NMAP removes that user from the local recipients list. When there are no more local recipients, the message is deleted or, if there are any Remote Recipients, the message is moved to queue 7 for remote delivery.

NOTE: NMAP always makes sure the destination is written before it deletes the source file, so in case the server goes down and transmission is interrupted, the message is not lost.

Data File Structure

When NMAP receives a message in the message queue, it saves that message as a data file. The data file is the actual message that is copied to the recipients' mailboxes. It contains the message

header, message text, and any attachments. Because most message processing is done through the control file, the data file is rarely opened.

SCMS Message Structure

In cases when a message is sent to multiple recipients (by default, five or more) and the message is over 5 KB, NMAP does not replicate the message in all the users' mailboxes. Instead, a pointer message is sent to the individual mailboxes directing NMAP to the complete message in the Single-Copy Message Store (SCMS) directory.

The following is an example of the message that is sent to the user's mailbox.The X-SCMS-ID, 181703758, is a decimal value that points NMAP to the corresponding message in the SCMS directory.

```
The following is a sample control file:

D995677347
Fadmin@test.com
X1
Riman@visioncorp.com iman@visioncorp.com 28
```

The SCMS directory contains the complete message and a counter file. The message and counter filenames are the hex equivalent of the SCMS-ID. In the case of the above pointer message, the message filename is 0AD4944E and the counter filename is 0Ad4944E.cnt.

The counter file stores a value equal to the total number of recipients. As each recipient deletes the message, the counter file decrements by 1. When the last user downloads or deletes the message, both the message and the counter file are deleted from the SCMS directory.

Mailbox File Structure

User mailboxes are comprised of two files: inbox.idx and inbox.box. If the user has an IMAP mail client, there are also .idx and .box files for each of the user's folders (for example, sent.idx and sent.box; personal.idx and personal.box, and so on).

The idx file is a binary index file. NMAP uses idx to locate messages in the corresponding box file. The idx file is initially created when the user first logs in to the messaging system. Thereafter, it is dynamically updated at each login.

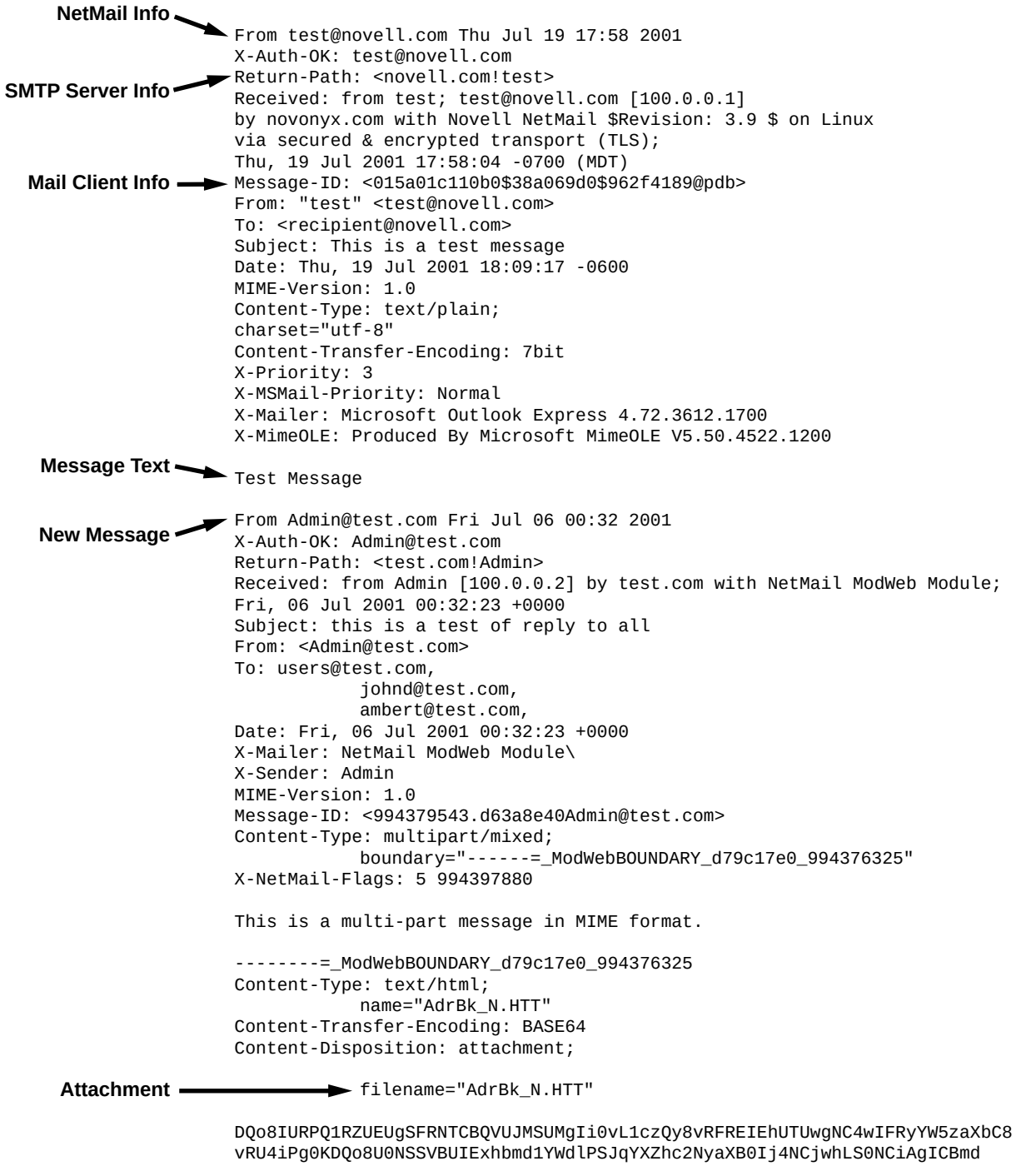
NOTE: If a user's mailbox ever becomes corrupted, see "Fixing Corrupt Mailboxes" on page 206.

For additional troubleshooting information, reference NetMail FAQ (http://www.novell.com/coolsolutions/netmail/features/a_nims_faq_nm.html).

The box file is a simple text file containing the user's messages. The message includes the message header (NetMail info, SMTP Server Info, and Mail Client Info), Message Text, and any attachments. When NMAP parses the box file to figure out where one message ends and the other begins, it looks for a blank line and the NetMail Info (the From and X-Auth lines). New messages are appended to the end of the file.

The following is a sample box file:

Description: Sample Box File




```
From test@novell.com Thu Jul 19 17:58 2001
X-Auth-OK: test@novell.com
Return-Path: <novell.com!test>
Received: from test; test@novell.com [100.0.0.1]
by novonyx.com with Novell NetMail $Revision: 3.9 $ on Linux
via secured & encrypted transport (TLS);
Thu, 19 Jul 2001 17:58:04 -0700 (MDT)
Message-ID: <015a01c110b0$38a069d0$962f4189@pdb>
From: "test" <test@novell.com>
To: <recipient@novell.com>
Subject: This is a test message
Date: Thu, 19 Jul 2001 18:09:17 -0600
MIME-Version: 1.0
Content-Type: text/plain;
charset="utf-8"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.3612.1700
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4522.1200

Test Message

From Admin@test.com Fri Jul 06 00:32 2001
X-Auth-OK: Admin@test.com
Return-Path: <test.com!Admin>
Received: from Admin [100.0.0.2] by test.com with NetMail ModWeb Module;
Fri, 06 Jul 2001 00:32:23 +0000
Subject: this is a test of reply to all
From: <Admin@test.com>
To: users@test.com,
            johnd@test.com,
            ambert@test.com,
Date: Fri, 06 Jul 2001 00:32:23 +0000
X-Mailer: NetMail ModWeb Module\
X-Sender: Admin
MIME-Version: 1.0
Message-ID: <994379543.d63a8e40Admin@test.com>
Content-Type: multipart/mixed;
            boundary="------=_ModWebBOUNDARY_d79c17e0_994376325"
X-NetMail-Flags: 5 994397880

This is a multi-part message in MIME format.

--------=_ModWebBOUNDARY_d79c17e0_994376325
Content-Type: text/html;
            name="AdrBk_N.HTT"
Content-Transfer-Encoding: BASE64
Content-Disposition: attachment;

            filename="AdrBk_N.HTT"

DQo8IURPQ1RZUEUgSFRNTCBQVUJMSUMgIi0vL1czQy8vRFREIEhUTUwgNC4wIFRyYW5zaXbC8
vRU4iPg0KDQo8U0NSSVBUIExhbmd1YWdlPSJqYXZhc2NyaXB0Ij4NCjwhLS0NCiAgICBmd
```

C Supported Standards

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.

NetMail fully supports the major Internet open standards because it complies with the current RFC definition. Compliance with these standards provides seamless messaging between NetMail and all e-mail clients that use these standards. This broad-based support eliminates the need for gateways and reduces file translation errors, all without degrading system performance.

This appendix lists all the standards supported by NetMail, their RFCs, and the specific Agents that use the stated protocol. It also provides basic explanations of the e-mail protocols and security standards.

Supported Standards

Table 10 Supported Standards

RFC	Title	Applies To
2821	Simple Mail Transfer Protocol (SMTP)	SMTP Agent
2822	ARPA Message Format	All Agents
1123	Requirements for Internet Hosts	All Agents
1157	Simple Network Management Protocol (SNMP)	All Agents
1213	SNMP Management Information Base (MIB)	All Agents
1215	SNMP Trap Conventions	All Agents
1426	8-bit SMTP Transport	SMTP Agent
1456	Vietnamese Character Message Encoding	Modular Web Agent
1468	Japanese Character Message Encoding	Modular Web Agent
1777	Lightweight Directory Access Protocol (LDAP)	Address Book Agent
1869	SMTP Extension Syntax	SMTP Agent
1870	SMTP Size Extension	SMTP Agent
1891	SMTP Delivery Status Notifications	SMTP Agent
1922	Chinese Character Message Encoding	Modular Web Agent

RFC	Title	Applies To
1939	Post Office Protocol Version 3 (POP3)	POP Agent
1985	SMTP Remote Message Queue Starting	SMTP Agent
2045	Multipurpose Internet Mail Extensions (MIME)	All Agents
2046	MIME Part II	All Agents
2047	MIME Part III	All Agents
2060	Internet Message Access Protocol (IMAP4rev1)	IMAP Agent
2195	POP3\IMAP4 Authentication Command	POP, IMAP
2197	SMTP Command Pipelining	SMTP Agent
2231	MIME Charsets, Languages, and Continuations	All Agents
2246	Transport Layer Security (TLS)	SMTP, POP, IMAP, Modular Web, WebAdmin Agents
2279	Unicode* Transformation Format (UTF-8)	Modular Web Agent
2311	Secure MIME (S/MIME)	SMTP, POP, IMAP Agents
2449	POP3 Extension Mechanism	POP Agent
	Secure Sockets Layer (SSL)	SMTP, POP, IMAP, Modular Web, WebAdmin Agents
PKCS 1-12	Public Key Cryptography Standards	SMTP, POP, IMAP, Modular Web, WebAdmin Agents
X.509v3	Client Certificates	SMTP, POP, IMAP, Modular Web, WebAdmin Agents
2445	Internet Calendaring and Scheduling Core Object Specification (iCalendar)	ModWeb Calendar Module
2447	iCalendar Message-Based Interoperability Protocol (iMIP)	ModWeb Calendar Module

Protocol Descriptions

POP3 and IMAP4

Supporting both Post Office Protocol 3 (POP3) and Internet Mail Access Protocol 4 (IMAP4) standards, NetMail is compatible with any client e-mail application including GroupWise, Microsoft Outlook Express, Netscape Communicator, Eudora, Pegasus, and other integrated or standalone e-mail clients. See “POP Agent” on page 77 and “IMAP Agent” on page 79.

SMTP

NetMail supports Simple Mail Transfer Protocol (SMTP), a protocol used to transfer messages from server to server. Because NetMail supports SMTP, it is compatible with e-mail servers on the

Internet and most TCP/IP systems, thereby providing native SMTP/IP routing. See "SMTP Agent" on page 89.

LDAP

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

LDAP compatibility means that you can integrate NetMail with any LDAP-compliant mail client to give users access to address book information in eDirectory. NetMail also enables users to access any LDAP compliant address book within Webmail or WebAccess.

NetMail supports a read-only subset of LDAP3 enabling it to perform address book queries. See "Address Book Agent" on page 106.

SSL

NetMail protects system integrity by supporting the Secure Sockets Layer (SSL) 3.1 protocol. Using SSL 3.1, NetMail secures e-mail transmissions, remote administration, and user authentication over the Internet. NetMail supports SSL on all protocols including POP3, IMAP4, SMTP, and HTTP. SSL was originally created by Netscape and, although it has become a de facto Internet standard, it is not an RFC standard.

For specific information on incorporating SSL in NetMail, see "Setting Up TLS and SSL" on page 231.

NOTE: TLS does not encrypt actual messages. Messages are encrypted using X.509 client certificates. These certificates are not installed or managed at the server level; you must install them through the e-mail client. For more information on installing X.509 client certificates, contact your e-mail client vendor.

TLS

TLS is the official Internet standard for transport encryption. TLS can run on the native or SSL ports for any supported protocol. NetMail allows POP, IMAP, and HTTP mail clients that support TLS to automatically switch into encrypted mode without switching ports.

Because TLS advertises itself in the initial SMTP exchange, mail servers that support TLS also have the ability to automatically switch into encrypted mode. If TLS is configured, NetMail messaging servers automatically switch into encrypted mode when communicating with other mail servers that support TLS.

For specific information on incorporating TLS in NetMail, see "Setting Up TLS and SSL" on page 231.

NOTE: TLS does not encrypt actual messages. Messages are encrypted using X.509 client certificates. These certificates are not installed or managed at the server level; you must install them through the e-mail client. For more information on installing X.509 client certificates, contact your e-mail client vendor.

HTTP

HyperText Transport Protocol (HTTP) support allows users to access their mailboxes from any standard Web browser. See "WebAdmin" on page 51.

HTTP support also enables Web-based administration. System administrators can manage NetMail's user and messaging configurations from any standard Web browser. See "WebAdmin" on page 51.

MIME and S/MIME

NetMail supports Multipurpose Internet Mail Extensions (MIME) for sending and receiving messages with rich content.

NetMail also supports S/MIME v3 for messages that are signed or encrypted with x.509 keys and certificates.

NOTE: The Modular Web Agent does *not* support S/MIME v3. Because it is a server-based client and you must store the x.509 private key on the server, it has the potential to compromise the key's security.

NMAP

Networked Messaging Application Protocol (NMAP) is an RFC-style protocol used to access user mailboxes and message queues in the NetMail messaging system. See "NMAP Agent" on page 67.

You can integrate additional functions such as fax, voice mail, and list servers with NetMail using NMAP-compliant applications.

iCalendar

The iCalendar protocol provides a common format for openly exchanging calendaring and scheduling information across the Internet. Applications that support the iCalendar provide interoperable calendaring and scheduling services for the Internet.

NetMail 3.5 supports iCalendar RFS 2445 and 2447. Consequently, you can use NetMail calendaring functions such as calendar events, tasks, notes, and even busy searches, in conduction with any iCalendar compliant application.

D Port Assignments

Before installing NetMail, check for duplicate port assignments on your server. If other programs on the server already use these ports, conflicts will occur.

The following table lists the default NetMail port assignments, their associated agents, and indicates whether you can configure the port assignment.

Standard NetMail Port	Novell Nterprise Linux Services	Protocol	Agent	Configurable Port
25	25	SMTP	SMTP Agent	no
80	52080	HTTP	Modular Web Agent	yes
443	52443	HTTPS	Modular Web Agent secure	yes
110	110	POP3	POP Agent	no
995	995	SSL over POP	POP Agent secure	no
143	143	IMAP4	IMAP Agent	no
993	993	SSL over IMAP4	IMAP Agent secure	no
389	52389	LDAP	Address Book Agent	yes
689 UDP	689 UDP	NMAP	NMAP Agent	no
			Connection Manager uses UDP port 689 to receive client IP addresses from the POP and IMAP Agents	
689 TCP	689 TCP	NMAP	NMAP Agent	no
89	8018	HTTP	WebAdmin Agent	yes
449	8020	HTTPS	WebAdmin Agent	yes
		TLS	NetMail supports TLS on every protocol's native port.	
1026	1026	CAP	Calendar Agent, CAP Agent, ModWeb Calendar Module (they all use CAP?)	no
NA	80	HTTP	Apache Web Server	yes
NA	443	HTTPS	Apache Web Server secure	yes
NA	8008	HTTP	eDir iMonitor	yes

Standard NetMail Port	Novell Nterprise Linux Services	Protocol	Agent	Configurable Port
NA	8010	HTTPS	eDir iMonitor secure	yes
NA	389	LDAP	eDir LDAP Server	yes
NA	636	LDAP (SSL)	eDir LDAP Server secure	yes
NA	631	IPP	iPrint IPP Server	yes
NA	443	IPP (SSL)	iPrint IPP Server secure	yes
NA	137	CIFS/SMB	Samba	yes
NA	138	CIFS/SMB	Samba	yes
NA	139	CIFS/SMB	Samba	yes
NA	8080	HTTP	Tomcat	yes
NA	8089	MOD_JK	MOD_JK	yes
524	524	NDAP	eDirectory	no
NA	1229	TED	ZfS	yes

NOTE: To change the port numbers the NetMail agents use, refer to the agent configuration options in “NetMail Agent Configuration Options” on page 359.

E Implementing Administrative Changes

When making administrative changes in NetMail™, there are varied time frames within which those changes are actually implemented. In some instances, NetMail immediately executes the changes. In other instances, changes are slightly delayed. Still others require that you restart the associated agent before the changes are put into effect.

NOTE: For information on restarting an agent, see "Loading and Unloading NetMail Agents" on page 317.

The following table outlines the implementation time frames associated with each NetMail property.

Table 11 Implementation Time Frames

Object	Page	Feature	Time Effective
Internet Services Container			
	Syslog Configuration	Log Level	After restarting IMS
		Log to file	After restarting IMS
Messaging Server			
	Identification	NetWare® Host	After restarting IMS
		PostMaster	After restarting IMS
		Official Domain	Within 5 minutes
		Temp Directory	After restarting IMS
		DBF Directory	After restarting IMS
Messaging Server *continued*			
		Resolvers	After restarting IMS
		Connection Manager	Within 5 minutes
		Distributed Processing Disabled	After restarting IMS
	Security	Enable SSL and TLS	After restarting IMS
		Server Managers	Immediately
	Statistics	Statistics	NA

Object	Page	Feature	Time Effective
	SNMP Configuration	Organization	After restarting IMS
		Location	After restarting IMS
		Contact	After restarting IMS
		Name	After restarting IMS
	Status	Advanced IP Options	Within 5 minutes
		Disable Server	After unloading IMS
Parent Object			
	Options	Default Inheritance	Immediately
		Object Description	Immediately
		Mail Availability	Immediately
	IMAP	IMAP Access	Immediately
	POP	POP Access	Immediately
	Forward	Forward Ability	Immediately
		Forward Mail To	Immediately
	AutoReply	Auto Reply Ability	Immediately
		Enable	Immediately
Parent Object *continued*			
	Messaging Rules	Rule Usage Ability	Immediately
	NMAP	Mailbox Quota	Immediately
		PostMaster	Immediately
		Mail Store	Immediately
	Task-Oriented Management	Managed Parent Objects	Immediately
		Managed Contexts	Immediately
		Maximum Users	Immediately
	ModWeb Mail	Size Limit	Immediately
		Maximum Recipients	Immediately
		Address Book	Immediately
	ModWeb Preference	Allow User to Change Password	Immediately
		SSL Required	Immediately
	Modular Web Agent	Modular Web Access	Immediately

Object	Page	Feature	Time Effective
		Identifier	Immediately
		Default Template	Immediately
		Available Templates	Immediately
		Default Timezone	Immediately
		Default Language	Immediately
	SMTP	Global Domains	Within 5 minutes
		Hosting Domains	Within 5 minutes
		Allowed Hosts	Within 5 minutes

Object	Page	Feature	Time Effective
Parent Object *continued*			
		ETRN Domains	Within 5 minutes
	Calendar Agent	Calendar Access	Immediately
	Mail Proxy	Proxy Access	Immediately
	Calendar/Scheduling	Calendar Access	Immediately
	AntiVirus	Virus Scanning	Immediately
Template			
	Options		NA
Mailing List			
	Configuration	Abstract	Immediately
		Description	Immediately
		Subscriptions	Immediately
		Review	Immediately
		Postings	Immediately
	Options	Plaintext Signature	Immediately
		HTML Signature	Immediately
		Keep Archive	Immediately
		Generate Digest	Immediately
	Signatures	Plaintext	Immediately
		HTML	Immediately
	NMAP Store	NMAP Store	Immediately

Object	Page	Feature	Time Effective
List User Object			
	General	Full name	Immediately
	Options	Receive list messages	Immediately
		Receive list digests	Immediately
		Send copy of own postings	Immediately
		Don't show user	Immediately
		Banned user	Immediately
		Postings require approval	Immediately
NDS Mailing List			
	Configuration	Abstract	Immediately
		Description	Immediately
		Senders	Immediately
		Members	Immediately
		Require senders to authenticate	Immediately
	NMAP Store	NMAP Store	Immediately
NMAP Agent			
	Parameters	Message Store	After restarting NMAPD
		Spool Directory	After restarting NMAPD
		Minimum Space	After restarting NMAPD
		SCMS Directory	After restarting NMAPD
	Queue Parameters	Retry Interval	Within 5 minutes
		Retry Timeout	Within 5 minutes
NMAP Agent *continued*			
	Options	Bounced Message Control	Within 5 minutes
		Forward Local Undeliverable	Within 5 minutes
		Remote Queue Restrictions	After restarting NMAPD
	Contexts	Contexts	Within 5 minutes
	Mailbox Quota	Per User Mailbox Quotas	After restarting NMAPD
		System-Wide Mailbox Quotas	After restarting NMAPD
		Quota Return Message	After restarting NMAPD

Object	Page	Feature	Time Effective
	Single Copy Message Store	Minimum number of recipients	Within 5 minutes
		Minimum Message Size	Within 5 minutes
	Status	Disable Agent	After unloading NMAPD
	Trusted Hosts	Trusted Hosts	Within 5 minutes
	Clients	Clients	NA
SMTP Agent	Identification	Global Domains	Within 5 minutes
		Hosting Domains	Within 5 minutes
		Message Size Limit	Within 5 minutes
	Options	Flags	Within 5 minutes
		Mail Relay Host	After restarting SMTPD
	UBE Blocking	Flags	Within 5 minutes
		RBL CheckList	Within 5 minutes
		Blocked Host	Within 5 minutes
SMTP *continued*			
	UBE Relaying	Flags	Within 5 minutes
		Maximum Recipients	Within 5 minutes
		Allowed Hosts	Within 5 minutes
		Relayed Domains (ETRN)	Within 5 minutes
	NetMail Parent Object	Parent Object List	Within 5 minutes
	Queue Server	NMAP Agent	After restarting SMTPD
	Monitored Queues	NMAP Agents	Within 5 minutes
	Status	Disable Agent	After unloading SMTPD
POP Agent			
	Status	Disable Agent	After unloading POP3D
IMAP Agent			
	Status	Disable Agent	After unloading IMAPD
Modular Web Agent			
	Configuration	Ports	After restarting MODWEBD
		Identifier	After restarting MODWEBD
		Templates	After restarting MODWEBD

Object	Page	Feature	Time Effective
		Default Timezone	After restarting MODWEBD
		Default Language	After restarting MODWEBD
	Status	Disable Agent	After unloading MODWEBD

Object	Page	Feature	Time Effective
MW Mail Module			
	Configuration	Limits	After restarting MODWEBD
		Address Book	After restarting MODWEBD
	Queue Server	NMAP Agent	After restarting MODWEBD
MW Calendar Module			
	Queue Server	NMAP Agent	After restarting MODWEBD
MW Preference Module			
	Configuration	Passwords	After restarting MODWEBD
MW Task Oriented Management			
	Information		NA
Address Book Agent			
	Configuration	Scheduler	After restarting MSGLDAP
		LDAP/LDIF	After restarting MSGLDAP
	Monitored Servers	NMAP Agents	After restarting MSGLDAP
	Status	Disable Agent	After restarting MSGLDAP
	Optional attributes	Require Authentication	After restarting MSGLDAP
		Derive Search Domain from Authentication	After restarting MSGLDAP
		Derive Search Domain from Authentication	After restarting MSGLDAP
		Require Search Domain	After restarting MSGLDAP

Object	Page	Feature	Time Effective
AutoReply Agent			
	Monitored Queues	NMAP Agents	After restarting FORWARD
	Status	Disable Agent	After unloading FORWARD
Rule Agent			
	Monitored Queues	NMAP Agents	After restarting RULESRV
	Status	Disable Agent	After unloading RULESRV
AntiVirus Agent			
	AntiVirus Engine	CAInoculateIT	After restarting AVIRUS
		McAfee	After restarting AVIRUS
		Pattern-file path	After restarting AVIRUS
		Symantec CarrierScan Server	After restarting AVIRUS
		Scanning	After restarting AVIRUS
		Behavior	After restarting AVIRUS
	Monitored Queues	NMAP Agents	After restarting AVIRUS
	Status	Disable Agent	After restarting AVIRUS
Proxy Agent			
	Configuration	Pick-Up Interval	After restarting MAILPROX
		Pick-Up Threads	After restarting MAILPROX
	Monitored Queues	NMAP Agents	After restarting MAILPROX
	Queue Server	NMAP Agent	After restarting MAILPROX
	Status	Disable Agent	After unloading MAILPROX

Object	Page	Feature	Time Effective
Alias Agent			
	Configuration	Scheduler	After restarting MSGALIAS
		Automatic Aliases	After restarting MSGALIAS
	Internet E-mail Address	Automatic Attribute Population	After restarting MSGALIAS
	Local Aliases	Local Aliases	After restarting MSGALIAS
	Global Aliases	Global Aliases	After restarting MSGALIAS
	Monitored Servers	NMAP Agents	After restarting MSGALIAS
	Status	Disable Agent	After restarting MSGALIAS
AntiSpam Agent			
	Configuration	Blocked Domains	After restarting ANTISPAM
		Send Back	After restarting ANTISPAM
		CC Postmaster	After restarting ANTISPAM
	Monitored Queues	NMAP Agents	After restarting ANTISPAM
	Status	Disable Agent	After unloading ANTISPAM
List Agent			
	Configuration	Create Digest Time	After restarting IMSLIST
	Monitored Queues	NMAP Agents	After restarting IMSLIST
	Status	Disable Agent	After unloading IMSLIST
Connection Manager Agent			
	Configuration	Expiration Time	After restarting GKEEPER
	Status	Disable Agent	After unloading GKEEPER

Object	Page	Feature	Time Effective
Server Object			
	Syslog Configuration	Log Level	After restarting IMS
		Log to file	After restarting IMS
		Do not log	After restarting IMS
		Override Global configuration	After restarting IMS
	NetMail Information		NA
Container Objects			
	NetMail Options	Message Store	Within 5 minutes
		Domain	Immediately
User Objects			
	All NIMS Options		Immediately

F NetMail Commands and Utilities

NetMail includes various commands and utilities that you can use to manage the messaging server and provide statistical information.

This appendix includes the following topics:

- "NetMail Startup Commands" on page 316
  - "Starting and Stopping NetMail on NetWare" on page 316
  - "Starting and Stopping NetMail on Windows" on page 316
  - "Starting and Stopping NetMail on Linux" on page 316
- "Loading and Unloading NetMail Agents" on page 317
  - "Loading and Unloading NetMail Agents on NetWare" on page 317
  - "Loading and Unloading NetMail Agents on Windows" on page 318
  - "Loading and Unloading NetMail Agents on Linux" on page 319
- "Secure Logging Server Startup Commands" on page 320
  - "Starting and Stopping the Secure Logging Server on NetWare" on page 321
  - "Starting and Stopping the Secure Logging Server on Windows" on page 321
  - "Starting and Stopping the Secure Logging Server on Linux" on page 322
- "Server Commands" on page 322
  - "MAIL (NetWare)" on page 322
  - "MAILCON (Windows)" on page 325
  - "NMAIL (Linux)" on page 326
- "Server Utilities" on page 328
  - "MAILCON" on page 328
  - "SYSLOG" on page 329
  - "IMSAUDIT" on page 330
  - "NIMSEXT" on page 332
  - "MAIL LOAD" on page 332
  - "RMBOX" on page 334

NetMail Startup Commands

NetMail startup commands start and stop the messaging server and its associated agents. The startup commands for NetWare®, Windows, and Linux systems are reviewed in the following sections.

Starting and Stopping NetMail on NetWare

After install, you must manually launch the messaging server on NetWare systems.

To launch NetMail 3.5, type **`load ims`** at the console prompt. Repeat this for every messaging server in the tree.

To stop NetMail, type **`ims u`** at the console prompt.

When starting NetMail, ims.nlm verifies that eDirectory™ is loaded and then launches the messaging server and its enabled agents with the exception of the WebAdmin Agent and the MAILCON utility. Ims.nlm does not load WebAdmin or the MAILCON utility. It will, however, unload these utilities to unload the messaging server. Ims.nlm is located in the sys:\system directory.

During installation, the autoexec.ncf file is updated to include the IMS command so that NetMail automatically loads each time you restart your server.

For information on starting individual agents, see "NetMail Agent Configuration Options" on page 359.

Starting and Stopping NetMail on Windows

After install, NetMail automatically launches on Windows systems.

To manually load or unload NetMail on Windows, you must start or stop the NetMail Manager service:

1. Click Start > Settings > Control Panel.
2. Open the Services window.
   - **2a** On Windows NT, select Services.
   - **2b** On Windows 2000 and XP, select Administrative Tools > Services.
3. In the list of installed services, right-click NetMailManager and select Start or Stop from the quick menu.

   Repeat this step for every messaging server in the tree.

For information on starting individual agents, see "NetMail Agent Configuration Options" on page 359.

Starting and Stopping NetMail on Linux

After install, NetMail automatically launches on Linux systems. To manually start or stop your NetMail system, use the following commands:

```
/etc/init.d/novell-netmail start
/etc/init.d/novell-netmail stop
```

For information on starting individual agents, see "NetMail Agent Configuration Options" on page 359.

The ims Executable

The novell-netmail script calls the /opt/novell/netmail/bin/ims executable, which functions as a monitor and auto-loader for your NetMail system. It monitors agents that are running and restarts them if needed.

You can use the following switches with the ims executable either in the NetMail script or on the command line:

Table 12 Linux IMS Switches

Switch	Description
-c *core_directory*	Specifies a directory for NetMail core files; core files named core.*time* are stored in *agent_name* subdirectories
-r	E-mails NetMail core files to the NetMail development team at Novell for analysis
-t *seconds*	Specifies the interval after which a stopped NetMail agent is automatically reloaded (unless the agent was killed with a -15)
-e *email_address SMTP_server*	Sends an error e-mail message to the specified e-mail address by way of the SMTP server specified by IP address or host name
-h	Displays this help information

Use the following kill commands with ims:

Table 13 Linux IMS Kill Commands

Command	Description
killall -15 ims	Unloads ims and all NetMail agents
killall -10 ims	Reloads any NetMail agents that were unloaded using killall -15
killall -12 ims	Disables agent monitoring; ims no longer reloads agents; core files and messages no longer are delivered.

Loading and Unloading NetMail Agents

The following sections provide the information needed to load and unload NetMail agents on NetWare, Windows, and Linux servers.

Loading and Unloading NetMail Agents on NetWare

To restart an individual agent on NetWare systems:

1. Stop the agent using the UNLOAD command.

   For example, **`unload nmapd`** .

2 Restart the agent using the LOAD command.

For example, **`load nmapd`** .

The following is a listing of the NLM program names for each NetMail agent:

Table 14 Loading and Unloading NetMail Agents on NetWare

Agent Object	Agent Name	NLM Program
	NMAP Agent	NMAPD.NLM
	SMTP Agent	SMTPD.NLM
	POP Agent	POP3D.NLM
	IMAP Agent	IMAPD.NLM
	Modular Web Agent	MODWEBD.NLM
	Address Book Agent	MSGLDAP.NLM
	AutoReply Agent	FORWARD.NLM
	Rule Agent	RULESERV.NLM
	Proxy Agent	MAILPROX.NLM
	Alias Agent	MSGALIAS.NLM
	AntiSpam Agent	ANTISPAM.NLM
	AntiVirus Agent	AVIRUS.NLM
	Calendar Agent	CALAGENT.NLM
	List Agent	IMSLIST.NLM
	Connection Manager	GKEEPER.NLM

Loading and Unloading NetMail Agents on Windows

To restart an individual agent on Windows systems:

1 Go to a DOS window and type nimsstop *program_name*

For example, **`nimsstop nmapd`** .

Ensure that you are in the \program files\novell\netmail\bin directory or have it in your path.

2 Restart the agent in the DOS window by typing the agent's program name.

For example, **nmapd** .

The following is a listing of the program names for each NetMail agent:

Table 15 Loading and Unloading NetMail Agents on Windows

Agent Object	Agent Name	Program Name
	NMAP Agent	NMAPD
	SMTP Agent	SMTPD
	POP Agent	POP3D
	IMAP Agent	IMAPD
	Modular Web Agent	MODWEBD
	Address Book Agent	MSGLDAP
	AutoReply Agent	FORWARD
	Rule Agent	RULESERV
	Proxy Agent	MAILPROX
	Alias Agent	MSGALIAS
	AntiSpam Agent	ANTISPAM
	AntiVirus Agent	AVIRUS
	Calendar Agent	CALAGENT
	List Agent	IMSLIST
	Connection Manager	GKEEPER

Loading and Unloading NetMail Agents on Linux

To restart an individual agent on Linux systems, kill the agent's process. The NetMail autoloader will then notice that a required agent is not running and will restart it for you.

To kill an agent's process, enter **killall -9 *agent_module_name*** .

For example **killall -9 nmapd** .

The following is a listing of the module names for each NetMail agent:

Table 16 Loading and Unloading NetMail Agents on Linux

Agent Object	Agent Name	Module Name
	NMAP Agent	nmapd
	SMTP Agent	smtpd
	POP Agent	pop3d
	IMAP Agent	imapd
	Modular Web Agent	modwebd
	Address Book Agent	msgldap
	AutoReply Agent	forward
	Rule Agent	ruleserv
	Proxy Agent	mailprox
	Alias Agent	msgalias
	AntiSpam Agent	antispam
	AntiVirus Agent	avirus
	Calendar Agent	calagent
	List Agent	imslist
	Connection Manager	gkeeper

Secure Logging Server Startup Commands

The Secure Logging Server (lengine) is the server component in the Nsure auditing system. It is installed on the server you want to manage the flow of information to and from the auditing system.

Lengine automatically loads MDB, the Directory interface. Before starting the logging server, MDB verifies Novell eDirectory™ is ready. If eDirectory is not ready, the logging server does not load.

NOTE: On Windows systems, the logging server does load, but it automatically falls back to Windows registry configuration.

The startup commands for NetWare, Windows, and Linux systems are reviewed in the following sections.

Starting and Stopping the Secure Logging Server on NetWare

On NetWare, the startup script for the Secure Logging Server is included in the auditsvr.ncf file. Auditsvr.ncf is added to the server's autoexec.ncf file during installation so lengine.nlm loads each time the server restarts.

To manually load the Secure Logging Server on NetWare, enter

```
load lengine
```

or

```
load auditsvr.ncf
```

If you want to prevent the Secure Logging Server from being unloaded by users with access to the server console, you can append the -n switch to the server startup script. (For example, load lengine -n .)

To manually unload the Secure Logging Server on NetWare, enter

```
unload lengine
```

NOTE: Lengine.nlm and auditsvr.ncf are located in the sys:\system directory.

You must individually start or stop each logging server in the tree.

Starting and Stopping the Secure Logging Server on Windows

On Windows, the startup script for the Secure Logging Server is included in the naudit.exe file. Naudit.exe has an Automatic startup type so lengine.exe loads each time the server restarts.

To manually load or unload the Secure Logging Server on Windows, you must start or stop the Novell Nsure Audit Manager service:

1. Click Start > Settings > Control Panel.
2. Open the Services window.
   - **2a** On Window NT, select Services.
   - **2b** On Windows 2000 and XP, select Administrative Tools > Services.
3. In the list of installed services, right-click Novell Nsure Audit Manager and select Start or Stop from the quick menu.

You must individually start or stop each logging server in the tree.

Starting and Stopping the Secure Logging Server on Linux

On Linux, the startup script for the Secure Logging Server is /usr/rc.d/init.d/naudit . This startup script loads lengine each time the server restarts.

To manually start the Secure Logging Server on Linux, enter

```
/usr/rc.d/init.d/naudit start
```

To stop the Secure Logging Server on Linux, enter

```
/usr/rc.d/init.d/naudit stop
```

You must individually start or stop each logging server in the tree.

Server Commands

Server commands perform a single function at the command line. They include

- “MAIL (NetWare)” on page 322
- “MAILCON (Windows)” on page 325
- “NMAIL (Linux)” on page 326

MAIL (NetWare)

The MAIL command is specific to NetWare systems. It provides monitoring and control of the message queue.

The following NetWare MAIL commands allow you to manage the message queue.

Table 17 NetWare MAIL Commands

Command	Description
MAIL STAT	Gives you a static snapshot of the messaging server’s statistics at a command prompt. You must type 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. Reported statistics are as follows: ◆ The number of local and remote messages that are 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 ModWeb Agents ◆ The total number of server connections; that is, the number of users and other messaging servers that are sending SMTP or ModWeb 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

Command	Description
MAIL STAT *continued*	◆ The number of failed messages ◆ The number of wrong passwords provided ◆ The number of unauthorized NMAP connections ◆ 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. For information on the MAILCON utility, see “MAILCON” on page 328.
MAIL QUEUE	Identifies the target domains for outbound messages and the number of messages going to those domains in the current server’s message queue. The information is written to QUEUE.IMS in the server /DBF directory. **NOTE:** Running MAIL QUEUE with the -e switch (MAIL QUEUE -e) opens QUEUE.IMS in the EDIT utility. This command is primarily a SPAM intervention option. When spammers are using your messaging server to relay or bounce SPAM, you are generally inundated with messages going to one or two domains. Using this command, you can identify the domains affected. You can then use the MAIL REMOVE command to delete those messages while they are still in the queue.
MAIL REMOVE *domain*	Removes all queued messages that are going to the specified domain. Use this command 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. MAIL SPAM also provides virus scanning statistics that require the AntiVirus Agent and a virus scanning engine.

Command	Description
	Anti-SPAM statistics include the following: • Bounces Refused corresponds to the Bounced Message Control option in the NMAP Agent's Parameters page. See the Bounced Message Control property in Table 4, "Configuring the NMAP Agent," on page 68. The reported value is the number of bounced messages previously deleted. Values vary on the NMAP Agent's bounced message threshold. • Access from Blocked Addresses corresponds to the Do Not Allow Access from Hosts in Blocked List option in the SMTP Agent's UBE Blocking page. See the Do Not Allow Access from Hosts in Blocked List property in Table 4, "Configuring the SMTP Agent," on page 91. 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. • Access Blocked Due to RBL List corresponds to the Check Against RBL List at Server option in the SMTP Agent's UBE Blocking page. See the RBL Check property in Table 4, "Configuring the SMTP Agent," on page 91. The reported value is the number of hosts on the RBL list that have attempted to connect with the current messaging server. • Remote Routing Attempts Denied corresponds to the Require Sender to Be in the Allowed List for Remote Sending option in the SMTP Agent's UBE Relaying page. See the Require Sender to Be in the Allowed List for Remote Sending property in Table 4, "Configuring the SMTP Agent," on page 91. 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. • Access Blocked Due to Missing DNS Entry corresponds to the Deny Access to Hosts Not in DNS option in the SMTP Agent's UBE Blocking page. See the Deny Access to Hosts Not in DNS property in Table 4, "Configuring the SMTP Agent," on page 91. The reported value is the number of hosts without valid DNS entries that have attempted to connect with the current messaging server.
MAIL SPAM *continued*	AntiVirus statistics include the following: • **Messages scanned**: the total number of messages scanned for viruses. • **Message-Attachments scanned**: the total number of message attachments scanned for viruses. • **Messages with Attachments blocked**: the total number of scanned messages with attachments that were blocked because they contained a virus. • **Messages with viruses found**: the total number of scanned messages that contained a virus. • **Messages with viruses blocked**: the total number of scanned messages that were blocked because they contained a virus. • **Messages with viruses cured**: the total number of scanned messages that contained a virus and were fixed. Currently, this feature is not implemented, so the value is always "0."

MAILCON (Windows)

On Windows systems, MAILCON provides a static snapshot of the messaging server's statistics at a command prompt. You must type the command again to update the statistics.

On Windows, MAILCON provides the same information as the NetWare commands, MAIL STAT and MAIL SPAM. Reported statistics include

- The number of local and remote messages that are 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 ModWeb Agents
- The total number of server connections; that is, the number of users and other messaging servers that are sending SMTP or ModWeb 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 number of failed messages
- The number of wrong passwords provided
- The number of unauthorized NMAP connections
- The total number of NMAP connections
- Bounces Refused corresponds to the "Bounced Message Control" option in the NMAP Agent's Parameters page. See the Bounced Message Control property in Table 4, "Configuring the NMAP Agent," on page 68.

  The reported value is the number of bounced messages previously deleted. Values vary on the NMAP Agent's bounced message threshold.
- Access from Blocked Addresses corresponds to the "Do Not Allow Access from Hosts in Blocked List" option in the SMTP Agent's UBE Blocking page. See the Do Not Allow Access from Hosts in Blocked List property in Table 4, "Configuring the SMTP Agent," on page 91.

  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.
- Access Blocked Due to RBL List corresponds to the "Check Against RBL List at Server" option in the SMTP Agent's UBE Blocking page. See RBL Check property in Table 4, "Configuring the SMTP Agent," on page 91.

  The reported value is the number of hosts on the RBL list that have attempted to connect with the current messaging server.
- Remote Routing Attempts Denied corresponds to the "Require Sender To Be in the Allowed List for Remote Sending" option in the SMTP Agent's UBE Relaying page. See the Require Sender to Be in the Allowed List for Remote Sending property in Table 4, "Configuring the SMTP Agent," on page 91.

  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.
- Access Blocked Due to Missing DNS Entry corresponds to the "Deny Access to Hosts Not in DNS" option in the SMTP Agent's UBE Blocking page. See the Deny Access to Hosts Not in DNS property in Table 4, "Configuring the SMTP Agent," on page 91.

The reported value is the number of hosts without valid DNS entries that have attempted to connect with the current messaging server.

- Messages scanned: the total number of messages scanned for viruses.
- Message-Attachments scanned: the total number of message attachments scanned for viruses.
- Messages with Attachments blocked: the total number of scanned messages with attachments that were blocked because they contained a virus.
- Messages with viruses found: the total number of scanned messages that contained a virus.
- Messages with viruses blocked: the total number of scanned messages that were blocked because they contained a virus.
- Messages with viruses cured: the total number of scanned messages that contained a virus and were fixed. Currently, this feature is not implemented, so the value is always "0."

NMAIL (Linux)

NMAIL provides a static snapshot of the messaging server's statistics at a command prompt. You must type the command again to update the statistics.

Before running NMAIL, you must run the following line:

```
export LD_LIBRARY_PATH=/opt/novell/netmail/lib:$LD_LIBRARY_PATH
```

IMPORTANT: Do not run NMAIL before the messaging server is loaded. Doing so offsets how server uptime is reported in subsequent NMAIL reports.

NMAIL provides the same information as the NetWare commands, MAIL STAT and MAIL SPAM.

NOTE: NMAIL SPAM does not include anti-virus statistics.

Table 18 Linux NMail Commands

Command	Description
NMAIL STAT	Gives you a static snapshot of the messaging server's statistics at a command prompt. You must type the command again to update the statistics. Reported statistics include ◆ The number of local and remote messages that are queued, received and delivered ◆ The total number of recipients of inbound and outbound messages

Command	Description
	◆ The total number of client connections; that is, the number of people logged in at that moment through the POP, IMAP, or ModWeb Agents ◆ The total number of server connections; that is, the number of users and other messaging servers that are sending SMTP or ModWeb 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 number of failed messages ◆ The number of wrong passwords provided ◆ The number of unauthorized NMAP connections ◆ The total number of NMAP connections
NMAIL SPAM	MAIL SPAM reports statistics that correspond to specific anti-SPAM features. Reported values are dependent on whether the associated properties are configured. MAIL SPAM also provided virus scanning statistics that require the AntiVirus Agent and a virus scanning engine. Anti-SPAM statistics include the following: ◆ Bounces Refused corresponds to the Bounced Message Control option in the NMAP Agent's Parameters page. See the Bounced Message Control property in Table 4, "Configuring the NMAP Agent," on page 68. The reported value is the number of bounced messages previously deleted. Values vary on the NMAP Agent's bounced message threshold. ◆ Access from Blocked Addresses corresponds to the Do Not Allow Access from Hosts in Blocked List option in the SMTP Agent's UBE Blocking page. See the Do Not Allow Access from Hosts in Blocked List property in Table 4, "Configuring the SMTP Agent," on page 91. 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.

Command	Description
	• Access Blocked Due to RBL List corresponds to the Check Against RBL List at Server option in the SMTP Agent's UBE Blocking page. See the RBL Check property in Table 4, "Configuring the SMTP Agent," on page 91. The reported value is the number of hosts on the RBL list that have attempted to connect with the current messaging server. • Remote Routing Attempts Denied corresponds to the Require Sender To Be in the Allowed List for Remote Sending option in the SMTP Agent's UBE Relaying page. See the Require Sender to Be in the Allowed List for Remote Sending property in Table 4, "Configuring the SMTP Agent," on page 91. 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. • Access Blocked Due to Missing DNS Entry corresponds to the Deny Access to Hosts Not in DNS option in the SMTP Agent's UBE Blocking page. See the Deny Access to Hosts Not in DNS property in Table 4, "Configuring the SMTP Agent," on page 91. 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 that you can run from the messaging server are as follows:

- "MAILCON" on page 328
- "SYSLOG" on page 329
- "IMSAUDIT" on page 330
- "NIMSEXT" on page 332
- "MAIL LOAD" on page 332
- "RMBOX" on page 334
- "SCMSMove" on page 335

An explanation of each utility follows.

MAILCON

NetWare systems use the MAILCON utility 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.

On NetWare systems, MAILCON dynamically updates the server data. Under Monitoring Options, you can configure the Statistics Details window to update every minute, every second, or every 10 seconds.

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 are 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 ModWeb Agents
- The total number of server connections; that is, the number of users and other messaging servers that are sending SMTP or ModWeb 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 the MAIL STAT property in Table 17, "NetWare MAIL Commands," on page 322.

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 provided
- The number of unauthorized NMAP connections

SYSLOG

IMPORTANT: NetMail 3.5 uses Novell Nsure Audit 1.0 to log messaging system activity. The SYSLOG utility is provided for backward compatibility only.

SYSLOG provides basic logging and report options that you can use to diagnose problems and fine-tune messaging server performance. The Messaging Server automatically launches SYSLOG every time it loads; however, you can also manually load SYSLOG at the command line before the messaging server tries to load it.

Configure the standard SYSLOG settings in the Internet Services and Server objects. For more information, see Table 29, "Internet Services Container," on page 343 and Table 4, "Server Objects," on page 393.

The following is a listing of the commands and switches you can use to manage SYSLOG at the command line:

Table 19 SYSLOG Commands

Command	Description
SYSLOG CONFIG	Identifies what log level is configured and the file names where the log messages are 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.

Table 20 SYSLOG Switches

Switch	Description
-l: <*directory*>	Sets the log directory.
-s: <*bytes*>	Sets the maximum log file size in bytes. The default is 1000000 (1 MB).
-r	Allows SYSLOG to roll. This means that rather than wrapping the log file when it reaches the maximum size, a new log file is created.
-a: <*days*>	Deletes log files that are older than the designated number of days.
-v	Displays the SYSLOG version.
-h -?	Displays SYSLOG help.

IMSAUDIT

All platforms use IMSAUDIT to count the total number of people who have logged in to the messaging system. This utility allows administrators to determine the total number of NetMail 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 NetMail licenses on a monthly, per-user basis. To get a complete record of user mailboxes, run IMSAudit on every server running the NMAP Agent (that is, every server that has a message store). On all platforms, the utility creates the IMSAUDIT.LOG file in the server's \DBF directory.

By default, IMSAUDIT provides the following data:

Table 21 IMSAudit Data

Item	Description
UserCount	Total number of users
Parent Count	Total number of Parent objects
Disabled	Total number of disabled User objects
Logged in	Total number of users who have logged in
Aged	Total number of days since account was last accessed
Forwarding	Total number of users forwarding mail
Vacation Reply	Total number of users that have a Vacation/Reply rule
Rules	Total number of rules
Proxies	Total number of proxy accounts
Aliases	Total number of Aliases
Spammers	This option is specific to MyRealBox.com and is not currently in use.

IMSAUDIT Parameters

You can run IMSAudit with several parameters. The command line syntax to run IMSAudit is

```
IMSAudit [-a:<days>] [-d] [-q] [-o:<options>] [-v] [-h | -?]
```

An explanation of the IMSAudit parameters is provided as follows:

Table 22 IMSAudit Parameters

Parameter	Description
-a:<days>	Counts accounts older than <days>.
-d	Creates a detailed Comma-Separated Value (CSV) report, which you can use to facilitate billing and account maintenance. By default, the IMSAUDIT.CSV file is stored in the server's \DBF directory. By default, -d provides all available information in the CSV report. You can narrow the report using the -o parameter.
-q	Causes IMSAudit to run in quiet mode.
-v	Displays IMSAudit version information.
-h | -?	Displays the IMSAudit Help screen.
-o:<options>	Sets reporting options for IMSAUDIT.CSV. Use this parameter in conjunction with -d.
<options>	
u	Reports the total number of users in the current messaging system.
f	Provides a report of all features for each user. A "0" value indicates the feature is not enabled. "1" indicates the feature is enabled.
w	Reports if each user has Message Forwarding enabled. A "0" value indicates the feature is not enabled; "1" indicates the feature is enabled.
v	Indicates if each user has Vacation Reply enabled. A "0" value indicates the feature is not enabled; "1" indicates the feature is enabled.
r	Indicates if each user has Rules enabled. A "0" value indicates the feature is not enabled; "1" indicates the feature is enabled.
l	Reports the date each user last logged in.
a	Indicates the total number of days since each user's account was last accessed.
p	Lists each user's associated Parent object.
x	Indicates if each user has Proxy enabled. A "0" value indicates the feature is not enabled; "1" indicates the feature is enabled.
n	Stores the IMSAudit data collected on each user in the associated User object's Novonyx:Accounting Data attribute. You can then use a DS editing tool, such as NDS Snoop, to view the data.
s	Reports the total mailbox space used for each user in bytes.

NIMSEXT

All platforms use the NIMSEXT utility to add or remove the NetMail schema from eDirectory.The installation program uses NIMSEXT to extend the eDirectory schema during initial installation.

NOTE: On Linux systems, the utility is nimsext.sh .

Under normal circumstances, extend the schema only one time. This is automatically done during the NetMail installation on the first server in the tree.

If, for some reason, the initial schema extension fails, you can use NIMSEXT to run the schema extension again. However, do not extend the schema again until the first schema extension is fully replicated.

NOTE: A common indicator that the NetMail schema extension has failed is when you create NetMail objects, but the objects don't get added to the tree. The problem is the tree doesn't know about the attribute, even though you are able to create the objects in WebAdmin.

In some instances, you can also use NIMSEXT to re-create objects in the tree. If the Internet Services, Template, Mailing List, or Parent containers are deleted from the tree, run NIMSEXT to re-create them.

To uninstall NetMail, simply run NIMSEXT to remove the directory schema and delete the program directories.

NOTE: For additional troubleshooting information, reference NetMail FAQ (http://www.novell.com/coolsolutions/netmail/features/a_nims_faq_nm.html).

MAIL LOAD

When server resources are abundantly available, the NMAP Agent attempts to instantaneously fulfill all mail requests. However, when the mail load is heavy, NMAP limits the number of threads for message delivery to preserve server resources.

Under normal conditions, NMAP creates two threads to deliver every message; one to receive the message and one to push the received message through the queue. This state is called Concurrent Mode.

When the number of delivery threads exceeds the Concurrent Limit, new threads both receive messages and push them through the queue. This state is called Sequential Mode.

When the number of threads exceeds the Sequential Limit, new threads receive messages, but defer delivery until the total number of threads drops back below the Concurrent Limit. Only when NMAP drops back into Concurrent Mode does it deliver queued messages.

When the NMAP Agent's Mail Load utility is enabled (by default) and the number of queued messages exceeds the trigger value, the Mail Load utility checks CPU utilization on a regular interval. If utilization exceeds the high threshold, NMAP lowers the Concurrent and Sequential Limits in an effort to lower utilization. If utilization drops below the low threshold, NMAP raises the Concurrent and Sequential Limits to ensure system resources are not wasted.

The MAIL LOAD command allows an administrator to observe and influence the NMAP Agent's load balancing settings. While load balancing functions without administrator interaction, an administrator can alter the MAIL LOAD settings to affect server performance.

MAIL LOAD Parameters

The MAIL LOAD utility is managed at the command line with the following parameters:

Table 23 MAIL LOAD Parameters

Parameter	Description
none	Displays a snapshot of the current server statistics: ◆ Limit Concurrent: the maximum number of delivery threads usable in Concurrent Mode. Thereafter, NMAP moves to Sequential Mode. This value fluctuates as moderated by the Mail Load utility. ◆ Limit Sequential: the maximum number of delivery threads usable in Sequential Mode. Thereafter, NMAP begins queueing messages. This value fluctuates as moderated by the Mail Load utility. ◆ Low utilization: the current low threshold for server utilization. ◆ High utilization: the current high threshold for server utilization. ◆ Interval: the interval that MAIL LOAD checks server utilization. ◆ Queue trigger: the current queue threshold. ◆ Thread load: the number of threads currently dedicated to message processing.
-l: low	Sets the low threshold for server utilization. The default value is 70%.
-h: high	Sets the high threshold for server utilization. The default value is 90%.
-i: seconds	Sets the interval that MAIL LOAD checks the server utilization. The default interval is 5 seconds.
-q: messages in queue	Sets the queue trigger. The queue trigger identifies the number of messages required in the queue before the monitor begins adjusting the concurrent and sequential limits. The monitor cannot adjust any parameters until the queue trigger is exceeded. The default value is 100 messages.
-r	Forces a queue restart. NMAP immediately tries to resend any messages in the queue when the total number of threads is below the concurrent limit. **NOTE:** NetMail never queues messages unless there is a problem. Under normal conditions, the NMAP Agent immediately tries to send messages after they are processed in the queue. If, for some reason, the message is not sent, it remains in the queue for the NMAP Agent's Retry Interval before NMAP tries to resend the message. This command bypasses the Retry Interval and forces the NMAP Agent to resend any messages in the queue.
-d	Disables the Load Monitor. It continues to monitor the NMAP Agent, but does not adjust any values in response to server utilization. The NMAP Agent continues operation at the current concurrent and sequential values.
-e	Enables the Load Monitor. By default, the Load Monitor is enabled.
-h	Displays a brief explanation of all MAIL LOAD parameters.

Configuration Examples

There are very few times when an administrator would need to override the MAIL LOAD default values; however, the following examples are instances in which it is practical to reconfigure the MAIL LOAD values.

- You can use MAIL LOAD to keep utilization down during server maintenance.

  The command, MAIL LOAD -h:12 -l:10 -t:10, causes NMAP to keep utilization between 10 and 12 percent while there are more than 10 queued messages.

- You can use MAIL LOAD to dedicate all possible resources to a bulk message delivery.

  The command, MAIL LOAD -h:99 -l:98, sets the High and Low thresholds to their upper limits.

  Typically, use this command when responsiveness to client requests is limited. For example, at night time.

RMBOX

IMPORTANT: Because you CANNOT undo an RMBOX action, use this utility with caution.

All platforms use RMBOX, a command line utility, to remove mailboxes and their associated directories and any associated SCMS files referenced in the mailstore. Use this utility in conjunction with IMSAudit to delete accounts not accessed in (x) number of days.

For a user to access and authenticate to the utility, you must designate the user as a server administrator.

NOTE: Server administrators are designated in the Security tab of the Messaging Server object. See "Configuring the Messaging Server" on page 63 for more information.

RMBOX Parameters

The command line syntax to run the RMBOX utility is

```
RMBOX -u:server_administrator -p:password {user | -f:user_list}
-l:log_file -c -s -d -v [-h | -?]
```

An explanation of the RMBOX parameters is provided as follows:

Table 24 RMBOX Parameters

Parameter	Description
-u:*server_manager*	The server manager's NetMail username. **NOTE:** For more information on server managers, see "Configuring the Messaging Server" on page 63.
-p:*password*	The server administrator's NetMail password.
user	An individual user's mailstore to be removed. Do not use this parameter with -f:<*userlist*>.
-f:*user_list*	A list of users' mailstores to be removed. The <*userlist*> must include a complete pathname. For example, volume:/path/filename

Parameter	Description
-c	In addition to removing the mailstore, removes the user(s) from eDirectory.
-d	Enables debug output.
-s	Stops RMBOX when an error is encountered.
-l:*logfile*	Logs RMBOX activity to the designated log file. On NetWare systems, the log file is stored in the sys: directory. On Windows, and Linux systems, the log file is stored in the current directory.
-v	Returns the RMBOX version.
-h | -?	Help

SCMSMove

If you are upgrading from NIMS 2.65 or earlier, you must update the SCMS directories on all messaging servers running NMAP agents.

IMPORTANT: Do not run NetMail when updating the SCMS directories.

To manually update the SCMS directories,

1. After installing NetMail 3.5, launch the SCMSMOVE utility,
   - On NetWare systems, enter **`load scmsmove`** at the server console.
   - On Linux systems, enter **`/opt/novell/netmail/bin/scmsmove`** at the server console.
2. Enter the current server's path to the SCMS directory.
   - On NetWare, the default path to the SCMS directories is sys:\novonyx\mail\scms .
   - On Linux, the default path to the SCMS directories is /var/opt/novell/netmail/scms/.

The SCMS messages found in this path are moved to the directory structure required by NetMail 3.5. The new SCMS directory structure enhances the NMAP Agent's performance in retrieving messages stored in the SCMS directories. (See "Single Copy Message Store Directory Structure" on page 21 for the new directory structure.)

G Optimizing a NetWare Server for NetMail

IMPORTANT: This appendix provides guidelines for fine tuning NetWare® servers running NetMail. The recommended value settings are guidelines to follow in fine-tuning your own messaging system. You must adjust these settings based on messaging traffic and the amount of memory available to your system.Reasonable values will depend on your network.

The following information helps you optimize NetMail performance on NetWare servers:

- "A Note About Fine Tuning Your Server" on page 337
- "Packet Receive Buffers" on page 337
- "Maximum Pending TCP Connection Requests" on page 338
- "Directory Caching Parameters" on page 338
- "File Caching Parameters" on page 340
- "Locking Parameters" on page 341
- "File System Parameters" on page 341
- "Small ECBs" on page 342
- "Disk Parameters" on page 342
- "Resetting Your NetWare Server" on page 342

A Note About Fine Tuning Your Server

This appendix provides guidelines for fine tuning NetWare servers running NetMail. The recommended value settings are guidelines to follow in fine-tuning your own messaging system. You must adjust these settings based on messaging traffic and the amount of memory available to your system. Reasonable values will depend on your network.

When fine tuning minimum and maximum settings, begin by setting the maximum way above what you think you need and set the minimum just below what you think you need, and then watch what happens. You want the value to change so you can see where it went. After monitoring the server's performance, adjust the settings to correspond with your observations. After the machine is tuned, the value is not expected to fluctuate.

Packet Receive Buffers

Any processed request uses a Packet Receive Buffer. This includes all NCP requests, SAPs, RIPs, TCP packets, etc. If the messaging server is bombarded with requests and there are not enough packet receive buffers, the system becomes bottlenecked and starts dropping requests. If a request

is dropped, the requester must re-send the request. Conversely, if you allocate too many packet receive buffers, they can potentially monopolize the server's resources.

Fine tuning these settings is a matter of allocating enough packet receive buffers to meet system demands, but capping them at the point of diminishing returns.

The Minimum Packet Receive Buffer setting pre-allocates the number of packet receive buffers the server automatically creates at boot time. Allocating packet receive buffers on the fly is a relatively slow process; therefore, pre-allocating the number of packet receive buffers normally required by your system optimizes server performance. Ideally, the Minimum Packet Receive Buffer setting represents the number of packet receive buffers your messaging server uses under normal conditions.

The Maximum Packet Receive Buffer setting is a high water mark; it sets a ceiling on the number of packet receive buffers allocated on the server. Setting a maximum protects the messaging server from using too much memory for Packet Receive Buffers. Ideally, set this parameter at the point that allocating any more packet receive buffers hinders, rather than helps the messaging system performance.

The ideal Packet Receive Buffer settings are as follows:

Table 25 Packet Receive Buffer Parameters

Parameter	Ideal Setting
Maximum Packet Receive Buffers	5000
Minimum Packet Receive Buffers	2000

IMPORTANT: These settings might require additional server memory. Packet receive buffers are roughly the size of your packets (1518 bytes for Ethernet) plus 500 bytes for a total of 2K. On a Token Ring network, packet receive buffers take approximately 4K. Consider your messaging server's available resources before setting these parameters.

Maximum Pending TCP Connection Requests

The Maximum Pending TCP Connection Requests setting determines the maximum number of simultaneous client/server requests the messaging server can accept. If the setting is too low, the server will drop connections. If the setting is too high, the connection buffers can potentially monopolize the messaging server's resources.

The default Maximum Pending TCP Connection Requests is 128. Ideally, set the setting high enough to accommodate the normal volume of client/server requests and low enough to protect the messaging server from allocating too many connection buffers.

NOTE: When a connection buffer is allocated, the memory is not released; therefore, in setting this parameter, consider how many connections you can buffer out.

Directory Caching Parameters

To maximize NetMail's performance on NDS, you can adjust the messaging server's directory caching parameters. Directory caching parameters impact the information about the file, not the information within the file.

The following table outlines the directory caching parameters and their ideal settings.

IMPORTANT: The ideal settings might require additional server memory. Consider your messaging server's available resources before setting these parameters.

Table 26 Directory Caching Parameters

Parameter	Set To	Ideal Setting
Minimum Directory Cache Buffers	The Directory Cache Buffers store file system directory information (i.e. the information about the file, not the information within the file.) The parameter pre-allocates the number of directory cache buffers the server automatically creates at boot time. Allocating directory cache buffers on the fly is a relatively slow process; therefore, pre-allocating the number of directory cache buffers normally required by your system reduces processor and I/O bottlenecks. **IMPORTANT:** Increasing this setting might require additional memory. Directory cache buffers are equivalent to the block size on disk (e.g. 64KB). So, to calculate the amount of memory used, multiply the number of directory cache buffers by the block size.	2000
Maximum Directory Cache Buffers	The Maximum Directory Cache Buffers setting is a high water mark; it sets a ceiling on the number of directory cache buffers allocated on the server. Setting a maximum protects the system from using too much memory for Directory Cache Buffers. Due to the fact that NetMail does a lot of file processing, the default Maximum Directory Cache Buffers setting does not give the system enough room to grow. Ideally, set this parameter as high as possible without impeding other server processes.	20,000
Dirty Directory Cache Delay Time	During large transactions, the messaging server writes file system information on partially received data to disk. Increasing this parameter forces the messaging server to wait a longer period of time before writing to disk. This not only reduces the number of disk transactions, but it makes the server write the data in larger chunks rather than a lot of little pieces. **NOTE:** This setting only impacts partially received information; the final transaction is always written to disk. Consequently, increasing this parameter only improves performance on large transactions.	10 seconds
Maximum Concurrent Directory Cache Writes	This parameter determines the number of threads the system can create at a given time to write file system data to disk. Limiting the number of potential threads conserves CPU; however, setting the value too low can create an I/O bottleneck.	500

Parameter	Set To	Ideal Setting
Directory Cache Allocation Wait Time	The amount of time the messaging server waits before allocating more directory cache buffers. When a cache buffer is allocated, it is not released unless the server is restarted. Therefore, assigning a wait time before a cache buffer is allocated protects server resources. Ideally, set the Directory Cache Allocation Wait Time long enough that you don't waste cache on a peak, but low enough that if you need it, you don't have to wait too long.	0.1 seconds
Directory Cache Buffer Non-Referenced Delay	This setting determines how often the Directory Cache buffer is refreshed. Every refresh requires a new disk read and write to memory. By increasing the value to 30 seconds, you decrease how often the refresh takes place. This setting decreases processor overhead and I/O traffic.	30 seconds
Maximum Number of Internal Directory Handles	This parameter determines the maximum number of files the messaging server can process simultaneously. Due to the fact that NetMail does a lot of file processing, the default setting is too restrictive. Ideally, set this parameter at the maximum value of 1000.	1000
Maximum Number of Directory Handles	This parameter determines the maximum number of files the messaging server can process simultaneously. Due to the fact that NetMail does a lot of file processing, the default setting is too restrictive. Ideally, set this parameter at the maximum value of 1000.	1000

File Caching Parameters

To maximize file system performance, you can adjust the messaging server's file caching parameters. File caching parameters impact the actual file rather than the directory information.

The following table outlines the file caching parameters and their ideal settings.

IMPORTANT: The ideal settings might require additional server memory. Consider your messaging server's available resources before setting these parameters.

Table 27 Caching Parameters

Parameter	Set To	Ideal Setting
Maximum Concurrent Disk Cache Writes	This parameter determines the number of threads the system can create at a given time to write files to disk. (i.e. the actual information in the file.) Limiting the number of potential threads conserves CPU; however, setting the value too low can create an I/O bottleneck.	4000

Parameter	Set To	Ideal Setting
Dirty Disk Cache Delay Time	During large transactions, the messaging server writes partially received files to disk. Increasing this parameter forces the messaging server to wait a longer period of time before writing to disk. This not only reduces the number of disk transactions, but it makes the server write the data in larger chunks rather than a lot of little pieces. **NOTE:** This setting only impacts partially received information; the final transaction is always written to disk. Consequently, increasing this parameter only improves performance on large transactions.	10 seconds

Locking Parameters

On network systems, the operating system must ensure that two or more applications do not attempt to modify the same file simultaneously. It does this by locking the file as soon as the first application opens it. All subsequent applications can read the file, but they cannot write to it until the first application is finished.

Due to the fact that NetMail does a lot of file processing, it requires a lot of file locks. Likewise, as NetMail interacts with eDirectory™ to retrieve configuration settings and user information, it requires a lot of record locks. Setting the locking parameters too low creates an I/O bottleneck and drags system performance. Ideally, set the locking parameters high enough the messaging server doesn't run into them, but low enough the system doesn't run away.

The ideal file and record locking settings are as follows:

IMPORTANT: The ideal settings might require additional server memory. Consider your messaging server's available resources before setting these parameters.

Table 28 Locking Parameters

Parameter	Ideal Setting
Maximum File Locks	20,000
Maximum Record Locks	100,000

File System Parameters

In processing messages, NetMail creates a lot of temporary files. If these files are not purged, they can quickly fill the volume and drag messaging system performance to a crawl.

To automate the process of purging NetMail's temporary files, enable the Immediate Purge of Deleted Files option using either the global switch in Monitor or by direct assignment using command-line utilities. Immediately purging deleted files accelerates server startup and improves message store performance; however, you lose the ability to restore deleted files on your volume.

NOTE: Instead of enabling immediate purge on the entire volume, you can apply this parameter to only the mail store directories. Limiting immediate purge to the NetMail mail store allows you to restore deleted files everywhere on your volume except the mail store directories.

IMPORTANT: You do not need to enable Immediate Purge of Deleted Files if you regularly purge NetMail's server volume. Depending on message traffic, you might need to purge NetMail's server volume on a weekly or a daily basis.

Small ECBs

The NetWare IP stack has a default limit of 1024 small ECBs (Event Control Blocks). When a server reaches this limit, the number of client connections grows abnormally high and the server starts dropping connections or data packets.

Under standard operating conditions, most NetMail servers require a higher small ECBs limit. Novell® recommends that you begin with a maximum small ECBs setting of 2048 on all NetMail servers. Then, if you experience problems with dropped connections or lost data, increase the setting.

NOTE: increasing the small ECBS limit requires additional RAM.

To override the default ECBS setting, type the following command near the end of the AUTOEXEC.NCF:

```
set tcp ip maximum small ecbs = 2048
```

Disk Parameters

If you have a battery backed up disk cache controller, you must turn on the Enable hardware write back option. (It is off by default). Otherwise, the messaging server will not take advantage of the cache on your disk controller.

Resetting Your NetWare Server

To activate any of the preceding options, you must reset the messaging server. To reset the server, type **`reset server`** and press Enter at the console prompt.

H NetMail Configuration

This Appendix compiles information presented in earlier sections to provide a centralized, "quick reference" for all configuration information.

NetMail configuration information is presented in the following categories.

- "NetMail Object Configuration Options" on page 343
- "NetMail Agent Configuration Options" on page 359
- "NDS Object Configuration Options" on page 393

NetMail Object Configuration Options

This section reviews the configuration options for the following NetMail Objects:

- Table 29, "Internet Services Container," on page 343
- Table 30, "List User Object," on page 344
- Table 31, "Mailing List Object," on page 345
- Table 32, "Messaging Server," on page 347
- Table 3, "NDS Mailing List Object," on page 351
- Table 4, "Parent Object," on page 352
- Table 3, "Template Object," on page 359

For an overview of each object's function, see "NetMail Components" on page 2.

Table 29 Internet Services Container

Option	Function
Pre-NetMail 3.5 Syslog	NetMail 3.5 uses Novell Nsure Audit to log messaging system activity. The syslog options in the Internet Services container are provided for backward compatibility only. For information on using Novell Nsure Audit to log messaging system activity, see Chapter 9, "Auditing Your Messaging System," on page 215. **IMPORTANT:** You must restart each messaging server to effect changes in the Internet Services' Syslog configuration. See "NetMail Startup Commands" on page 316 for more information.
Log Level	The Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug options represent messaging server events. Mark the events you want Syslog to track.

Option	Function
Log to file	Mark Log to file to write Syslog events to file. On NetWare® systems, the default path and filename is sys:\ETC\SYSLOG. If a filename is specified in the log file field, the designated file is created in the sys:\ETC\SYSLOG.D directory on every messaging server in the tree. If a full path and filename are specified, the designated file and directory structure is created on every messaging server in the tree. On Windows systems, the default path and filename is <*windows directory*>\ system32\drivers\etc\syslog. If a filename is specified in the log file field, the designated file is created in the <*windows directory*>\ system32\drivers\etc\ directory on every messaging server in the tree. If a full path and filename are specified, the designated file and directory structure is created on every messaging server in the tree. On Linux, Syslog is part of the operating system. It is typically configured by editing the /etc/syslog.conf file. The maximum Syslog file size is 1 MB. When the file exceeds 1 MB, it wraps.
Disable logging	If marked, no log file is created.

Table 30 **List User Object**

Option	Function
Configuration	
General	
Full name	The user's full name.
Options	
Send Each Message Posted to List	The current user receives all messages sent to the list. This property is the equivalent of the **`Set list_name Mail | NoMail`** command.
Send List Digests	The current user receives a digest of messages sent to the list. This property is the equivalent of the **`Set list_name Digest | NoDigest`** command. Mailing list digests are compilations of the messages broadcast through a mailing list in a 24-hour period. Digests have a table of contents in the body of the message and mailing list messages are included as attachments. The List Agent generates and distributes digests on a daily basis.
Send Messages Posted by Self	Copies the user on all his or her postings to the mailing list. This property is the equivalent of the **`Set list_name Repro | NoRepro`** command.
Send Confirmation of Postings	

Option	Function
Exclude User When Membership Lists Are Requested	Hides the user's full name and e-mail address. When someone requests the list's member information using the **`Review list_name Detailed`** or **`Lists Detailed`** commands, the current user's information does not appear. This property is the equivalent of the **`Set list_name Conceal | NoConceal`** command.
Restrictions	
Messages Must Be Approved Before Posting	A mailing list moderator must approve the current user's postings. (For more information, see the Moderators property in Table 5, "Configuring a Mailing List," on page 274.) This property is the equivalent of the **`Set list_name Verify | NoVerify`** command.
Ban user from list	The current user cannot post to the mailing list. This property is the equivalent of the **`Set list_name Ban | NoBan`** command.

Table 31 Mailing List Object

Option	Function
Configuration	
Abstract	A description of the mailing list that is included in the welcome message sent to users when they subscribe to the list.
Description	A detailed description of the mailing list. The mailing list description is returned when a user sends a **`review listname detailed`** command to the List server. See "User Commands" on page 280 for a complete list of commands.
Moderators	The user(s) assigned to moderate the mailing list. A list user is required. Moderators can perform the following mailing list functions: ◆ Manage and change attributes in the mailing list object by sending commands through their mail client. ◆ Add and delete users from the list in bulk. ◆ Receive messages to be moderated. (See the moderated property in Table 5, "Configuring a Mailing List," on page 274 for information on moderated lists.) **NOTE:** Moderators CANNOT create lists.

Option	Function
Keep Archive	Archives all messages sent to the mailing list. Archived messages are kept in an archive folder in the mailing list's mailbox. (See the NMAP Store property in Table 5, "Configuring a Mailing List," on page 274 for information on the mailing list mailbox.) For practicality and convenience, you can search archived messages. Messages are not put in the archive folder until after the digest is created. If the Generate Digest option is not selected, messages are sent directly to the archive folder.
Generate Digest	Generates a digest of all messages sent to the current Mailing List object. This option allows users to subscribe to a mailing list digest instead of receiving mailing list messages individually. Mailing list digests are compilations of the messages broadcast through a mailing list in a 24-hour period. Digests have a table of contents in the body of the message and mailing list messages are included as attachments. The List Agent generates and distributes digests on a daily basis. (See the Create Digests Daily at ____ hours property in Table 3, "Configuring the List Agent," on page 270 for more information.)
Options	
Subscriptions	
Open	Anyone can subscribe to the mailing list.
By Owner Only	Users must apply to a list moderator for membership. Only the moderator can add members to the list.
Closed	Only the NetMail administrator can add members to the mailing list.. **NOTE:** Mailing List moderators cannot add members to a closed list.
Review	
Public	Anyone can query information about the list. (See "User Commands" on page 280 for a complete list of query commands.)
Private	Only list members can query information about the list. (See "User Commands" on page 280 for a complete list of query commands.)
By Owner Only	Only moderators can query information about the list. (See "User Commands" on page 280 for a complete list of query commands.)
Posting	
Posting Accepted From:	
Members Only	
Anyone	Anyone can send messages to the mailing list.

Option	Function
Moderated Members	All messages addressed to the mailing list are first sent to the moderator. The moderator can make changes before posting the message to the mailing list. To post the message, the moderator simply forwards the message to the list. Rather than moderating all messages sent to the mailing list, you can choose to only moderate messages from specific users by selecting Postings require approval in the List User configuration. (See "List User Objects" on page 277 for more information.)
Moderators Only	Only the moderator can send messages to the mailing list.
Allow Messages with Attachments	Determines if mailing list messages may include attachments. If attachments are not allowed, messages with attachments are bounced.
Use List Address as Reply-To Address	If Yes, reply messages are sent to everyone in the mailing list. If No, reply messages are only sent to the original sender.
Signatures	
Plaintext Signature	If enabled, appends the plain text signature to every plaintext message sent to the mailing list.
HTML Signature	If enabled, appends the HTML signature to every HTML message sent to the mailing list.
Signatures	
Plaintext	The signature that is automatically appended to plain text messages.
HTML	The signature that is automatically appended to HTML messages. The signature can include HTML formatting codes.
Message Store	The NMAP message store that contains the mailing list mailbox. The mailbox contains the mailing list's digest and archive files. (This is only used if you select archive or digest options.) Use the Browse button to select the NMAP Agent you want to manage the mailing list's mailbox.

Table 32 Messaging Server

Option	Function
Identification	
Host Server	The full NDS context name of the messaging server. The host is selected when creating the Messaging Server object. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option	Function
PostMaster	The user assigned to manage the messaging server. This user can also receive copies of bounced messages. (See the CC PostMaster property in Table 4, “Configuring the NMAP Agent,” on page 68.) Click the browse button to select the PostMaster in the Directory tree. **IMPORTANT:** The PostMaster must belong to a Global Domain. You cannot designate Hosting Domain users as the messaging server PostMaster. For more information on Global and Hosting Domains, see “Global Domains” on page 248 and “Hosting Domains” on page 250 **IMPORTANT:** Do NOT delete the User object designated as the messaging server postmaster. You must reassign the PostMaster before deleting an existing PostMaster User object. Deleting the Postmaster’s User object changes Messaging Server object to type “Unknown.” Consequently, the Messaging Server object appears with a “?” in NDS. To reset Messaging Server object type, you must run the IMSPMFIX utility. You can download this utility at http://www.novell.com/coolsolutions/netmail/features/a_product_updates_nm.html. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)
Official Domain	The Internet domain serviced by the current messaging server (such as abc.com or 123.net). All system messages, such as those sent to the Postmaster, use this domain. Additionally, if the messaging server is running the NMAP Agent, the Official Domain Name is the default domain for users within the NMAP Agent’s context. **IMPORTANT:** For the Official Domain, a Global Domain is required; a Hosting Domain is not allowed. For more information on Global and Hosting Domains, see “Global Domains” on page 248 and “Hosting Domains” on page 250. You must register the Official Domain Name in DNS before the messaging system can send and receive mail via the Internet. NetMail can share an Internet domain with other messaging systems. NetMail can 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 “Domain Sharing” on page 251. Changes to this property are effective within 5 minutes.
Temp Directory	The volume and, optionally, the directory where NetMail agents write temporary files. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See“Loading and Unloading NetMail Agents” on page 317 for more information.)

Option	Function
DBF Directory	The volume and, optionally, the directory where the NetMail alias database, address book, and queue client files are stored. The queue client files track every NetMail agent that has registered with NMAP so, if the NMAP server goes down, the NMAP Agent can re-establish its client connections. Queue client files are most pertinent in distributed environments where NMAP clients can reside on different messaging servers than the NMAP Agent. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Resolver(s)	The IP address of one or more DNS servers that resolve host names into IP addresses. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See"Loading and Unloading NetMail Agents" on page 317 for more information.)
Distributed Processing	Determines if the messaging server interacts with other messaging servers in the Internet Services container using the NMAP protocol. Marking Disabled creates a standalone messaging server; that is, the messaging server no longer searches the Directory tree and its associated messaging servers for Internet Services. By default, Distributed Processing is enabled. This means that all messaging servers search the Directory tree for other messaging servers in Internet Services, even those created outside the Internet Services container. Therefore, you must mark Disabled to create a standalone messaging server, even if it is created outside Internet Services. **NOTE:** For help in determining whether distributed or standalone messaging servers best suit your messaging system environment, see "Selecting Your NetMail System Configuration" on page 28. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Connection Manager	If enabled, enter the full NDS context name of the server running the Connection Manager. You must have a Connection Manager running in your messaging system to configure this option. **IMPORTANT:** For Connection Manager to have a comprehensive record of all authenticated users, you can only have one Connection Manager per messaging system. Connection Manager tracks the IP addresses of authenticated users. If this field is completed, any agent running on the current messaging server can query the Connection Manager Agent to verify that a user has authenticated with the system. For example, the SMTP Agent utilizes the Connection Manager Agent for SMTP-after-POP authentication. Changes to this property are effective within 5 minutes. **NOTE:** For more information, see "SMTP-after-POP" on page 232 or "Connection Manager" on page 243.

Option	Function
Security	NetMail supports Secure Socket Layer (SSL) security. SSL secures information passed between mail clients and the messaging server through public key encryption. SSL does not secure messages leaving your mail system nor does it secure message content. However, you can use TLS to encrypt server-to-server Internet communications as long as both sides of the transaction support TLS. **NOTE:** To secure message content, users must have an X.509 certificate. To enable SSL and TLS, you must first have a server certificate installed on your messaging server. For information on setting up your server certificate, see "Setting Up TLS and SSL" on page 231.
SSL and TLS	Enabling SSL and TLS option allows mail clients to connect to the messaging server over an SSL or TLS connection. It also enables the messaging server to automatically switch into encrypted mode when communicating with other TLS-enabled mail servers. You must have a server certificate installed on your messaging server before you can enable this option. See"Setting Up TLS and SSL" on page 231 for more information. **IMPORTANT:** You must restart IMS to effect any changes in this property. (See"Loading and Unloading NetMail Agents" on page 317 for more information.)
Server Managers	Users who are given rights to access NetMail administrative utilities like RMBOX. The designated users must authenticate to these utilities by providing their NetMail username and password. For more information on the RMBOX utility, see
Statistics	The Statistics page is only available on NetWare servers. It provides up-to-date resource and performance statistics for a NetWare server—essentially the same statistical information as the MAILCON utility. This page is useful to those 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 are 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 Modular Web Agents ◆ The total number of server connections; that is, the number of SMTP, WebAccess, 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

Option	Function
Statistics *continued*	If the server is down, the statistics fields display “n/a.” For comprehensive statistical reports on NetWare and Windows servers, launch MAILCON. On Linux systems, run NMAIL. For more information on these commands and utilities, see Appendix F, “NetMail Commands and Utilities,” on page 315.
SNMP Configuration	Because NetMail supports SNMP (Simple Network Management Protocol), allowing you to use management tools such as HP OpenView or Novell ManageWise to detect problems, optimize server performance, and obtain long-term trending information. Provides organization, location, contact, and name information for the messaging server to pass to SNMP applications that request information about the messaging server. You must restart IMS to effect any changes in this property. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)
Status	Displays the IP address of the messaging server and its current status.
Force IP Address	If enabled, forces the messaging server to be associated with a specific IP address. Changes to this property is effective within 5 minutes.
Force Agents to Bind to Specified Address Only	If enabled, forces NetMail agents running on other messaging servers use the designated IP address to communicate with the current messaging server. This option is useful for clustering applications, such as Novell Clustering Services (NCS), that use secondary IP addresses. Changes to this property is effective within 5 minutes.
Server Status	By default, the messaging server is enabled. To disable the messaging server, 1. Mark Disable Server. 2. Click OK. Marking Disable Server prevents the messaging server from launching at server startup. However, to immediately disable the messaging server, you must manually unload IMS.NLM or restart the server. For more information on unloading the messaging server, “NetMail Startup Commands” on page 316. After the messaging server is disabled, the server does not launch IMS.NLM again until you deselect the Disable Server option and restart the server.

Table 3 NDS Mailing List Object

Option	Function
Configuration	Changes to the NDS Mailing List configuration are implemented immediately.
General	

Option	Function
Abstract	A description of the mailing list that is included in the welcome message sent to users.
Description	A detailed description of the mailing list. The mailing list description is returned when a user sends a **`review list_name detailed command`** to the List server. See “User Commands” on page 280 for a complete list of commands.
Senders	One or more users who are authorized to send to this NDS mailing list. Senders must belong to the local messaging system. Click the Browse button to select one or more senders in the Directory tree.
Members	The NDS objects belonging to the mailing list. You can include on NDS Mailing Lists: User objects, Groups, Aliases, Organizational Roles, or Container objects.
Options	
Require Sender to Authenticate via SMTP	Mark this option to require users to authenticate with the messaging system before sending to the mailing list. Users can authenticate through SMTP or send the message through the Modular Web Agent client. Requiring SMTP authentication ensures that anyone sending a message to the NDS mailing list is who they say they are. This prevents unauthorized users from sending to the list.
NMAP Store	The NMAP message store that contains the mailing list mailbox. The mailbox contains the mailing list’s digest and archive files. (This is only used if you select archive or digest options.) Use the Browse button to select the NMAP Agent you want to manage the mailing list’s mailbox.

Table 4 **Parent Object**

Option	Function
Options	Changes to these properties are implemented immediately.
Description	Text provided in this field displays in the TOM administrator interface. You can use this field to provide information or instructions for the TOM administrator.
Default Inheritance	Determines precedence. If there are conflicting configurations between the Parent and User objects, you can specify which object you want to take precedence.
Parent First	User object settings take precedence over the Parent object settings. If the User setting is not configured, the Parent setting is used.
User First	Parent object settings take precedence over the User object settings. If the Parent setting is not configured, the User setting is used.
Featires	Changes to these properties are implemented immediately.

Option	Function
IMAP	Allows the administrator to enable or disable IMAP connections for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
POP	Allows the administrator to enable or disable POP connections for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
Forwarding	Allows the administrator to enable or disable messaging forwarding for users associated with the current Parent object. If Enabled is selected, the Parent object's Forwarding settings are in effect for all users associated with the Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
AutoReply	Allows the administrator to enable or disable autoreply messaging for users associated with the current Parent object. If Enabled is selected, the Parent object's AutoReply/Vacation settings are in effect for all users associated with the Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
Messaging Rules	Allows the administrator to enable or disable the Rules feature for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
WebMail	
Modular Web Agent	Allows the administrator to enable or disable the Modular Web client for users associated with the current Parent object. If Enabled is selected, the Parent object's Modular Web Agent settings are in effect for all users associated with the Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
Proxy	Enables or disables the user's ability to proxy other e-mail accounts. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the calendar and scheduling options are enabled.
Calendar/Scheduling	Enables or disables the user's Calendar(s) and scheduling functions. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the calendar and scheduling options are enabled.
Calendar Access	Allows the administrator to enable or disable iCal functionality, including automatic event status tracking, for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.

Option	Function
AntiVirus	Allows the administrator to enable or disable virus scanning options for users associated with the current Parent object. Selecting Deferred defers the setting to the User object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
Internet Mail	Changes to these properties are implemented immediately.
Forwarding	
Enabled	Forwards all messages received by users associated with the current Parent object to the designated e-mail address. Use this option to provide relaying services for remote messaging systems. For details, see "Using Message Forwarding as an Alternative to ETRN" on page 252.
Enabled and Keep Local Copy	Enables Forwarding and keeps a copy of all forwarded messages in the users' mailboxes. If Keep Local Copy is not marked, incoming messages are simply forwarded; they are not delivered to the users' mailboxes.
Disabled	Disables message forwarding as configured in the Parent object. This does not disable the Forwarding feature in WebAccess or WebMail.
Forward To	The e-mail address to which incoming messages are forwarded.
Auto Reply	
Enabled	Sends the defined autoreply message in response to all messages received by users associated with the current Parent object. The autoreply message is only sent to the original sender; not all message recipients.
Disabled	Disables Auto Reply as configured in the Parent object. This does not disable the Auto Reply feature in WebAccess or WebMail.
Message	The auto reply message.
Quota Parameters	
Use If Specified Below, Fallback to User	Uses the mailbox quota configured in the Parent object. If no mailbox quota is configured in the Parent object, the setting defers to the mailbox quota defined in the User object.
Disabled	Disables all mailbox quotas for users associated with the current Parent object. This includes mailbox quotas configured in the Parent object, User object, or NMAP Agent.
Use User Values, Fallback to Values Below	Uses the mailbox quota configured in the User object. If no mailbox quota is configured in the User object, the setting defers to the mailbox quota defined in the Parent object.
Per User Mailbox Quota	If enabled, this is the mailbox quota applied to all users associated with the current Parent object. Type the maximum mailbox size in the kByte field. Messages, folders, and calendar items count against the mailbox quota.

Option	Function
TOM	Allows the administrator to give selected users rights to create, import, modify, or delete user accounts in the contexts and domains designated in the current Parent object. For more information, see "Task-Oriented Management" on page 262. **NOTE:** The rights to create, import, modify, or delete user accounts are granted in the User object under the Task-Oriented Management property. (See Table 5, "User Objects," on page 394 for more information.) These properties only apply to TOM administrators associated with the current Parent object. All changes to Task-Oriented Management properties are implemented immediately. **NOTE:** All task-oriented management functions are enabled by the Modular Web Agent Task Management Module. Although the module itself has no configurable options, to provide TOM functionality via WebAccess, it must run on the messaging server.
Managed Domain Names	The Hosting Domains which TOM administrators can select when creating new user accounts. The usernames for new Hosting Domain accounts include the selected domain's name (name@hosted_domain). See "Hosting Domains" on page 250 for information on Hosting Domain usernames.
Managed Domain Names *continued*	If this field is left blank, the domain defaults to the messaging system's Official Domain as defined in the messaging server configuration. Therefore, the default Internet e-mail address for new Global Domain accounts is username@official_domain. However, due to the nature of how Global Domains are handled in NetMail, you can actually address these users at any of the messaging system's Global Domains. See "Global Domains" on page 248 for more information on how Global Domain addressing works. **IMPORTANT:** If you type any domain in this field, NetMail assumes it is a Hosting Domain and all new users are created with a corresponding username (name@hosted_domain). **IMPORTANT:** The TOM module does verify the listed domains are valid Hosting Domains. To ensure a valid Hosting Domain, you must include the domain in either the SMTP Agent's or the Parent object's Hosting Domains lists. If the Hosting Domain is listed under the Parent object, you must include the Parent object in the SMTP Agent's list of NetMail Parent Objects. If the TOM administrator selects multiple Hosting domains when creating the user, the User object is created with the first domain name and Alias objects are created with the subsequent domain names. For example, if the TOM administrator selects domains abc.com and 123.com when creating a user account for jotero, the User object is created as jotero@abc.com. The Alias object, jotero@123.com, points to jotero@abc.com.
Managed Contexts	The NMAP context(s) in which TOM administrators can create, modify, delete, or import user accounts. If multiple contexts are selected, NetMail equally distributes User objects among the contexts.

Option	Function
Maximum Number of Allowed Users	The number of users that any TOM administrator can create associated with the current Parent object.
ModWeb Mail	Changes to this property are implemented immediately.
Limits	
Maximum Number of Recipients per E-mail	The maximum number of recipients for messages sent by users associated with the current Parent object.
Message Size LImit	The maximum size of messages that users can send associated with the current Parent object.
Address Book	
Personal	Enables users associated with the current Parent object to create personal address books. Users' personal address books are stored in their NDS User object. Consequently, users can access their personal address book from any location as long as they are logged in to the network.
System-Wide	If marked, this option gives users associated with the current Parent object access to a system-wide address book in the Modular Web client (WebAccess or Webmail). In the LDAP URL field, you can type the following LDAP parameters: ldap://user:password@hostname:port/?basedn ◆ The *user:password* variable is the user's name and password. ◆ *Hostname* identifies the LDAP server's host name or IP address. If you type the IP address of a server running the Address Book Agent, users can access address book information from eDirectory. ◆ *Port* specifies the LDAP port assignment. If the LDAP server uses the default LDAP port (port 389), you do not need to specify a port. ◆ *Basedn* identifies the address book context. This is required if the Require DN attribute is added to the Address Book Agent. It is ignored if the Derive DN from Authentication is added to the Address Book Agent. (See "Address Book Agent Optional Features" on page 110 for more information.) Users with the Privacy attribute set to Limited or None in their NDS User object are visible to other NetMail users in the System-Wide Address Book. Users with an Unlisted privacy setting are not visible in the System-Wide Address Book. **NOTE:** For information on providing domain-specific address books, see "Managing Multiple Address Books" on page 258.

Option	Function
Default LDAP Server	If marked, this option allows users associated with the current Parent object to define their own public address books in the Modular Web client (WebAccess or Webmail). To define a default Public LDAP Server, type the host name or IP address of any public LDAP server in the LDAP URL field. You can use the same LDAP parameters discussed under "System-Wide LDAP Server " **NOTE:** Users can designate a different Public address book in the Modular Web client interface.
ModWeb Preferences Module	Changes to this property are implemented immediately.
Password Settings	
Allow Change	Enables users associated with the current Parent object to change their NDS password in the Modular Web client (Webmail or WebAccess). Because NetMail is completely integrated with NDS, the only password it recognizes is the user's NDS password. Therefore, marking this option actually gives users rights to change their NDS password, regardless of whether they have rights to the actual password property in their NDS User object.
Require SSL	Requires an SSL connection between the Modular Web client and the messaging server before users associated with the current Parent object can change their password.
Disable Options	Disables user configuration options in the WebAccess and Webmail templates. If marked, these options do NOT appear in the User Preferences menu.
Timeout	The amount of idle time before the user is automatically logged out of the Modular Web client.
Colors	Template color definition options. This option is specific to the Webmail template.
Privacy	The user's level of privacy within the messaging system. The privacy level controls what the Address Book Agent reveals about the user.
Signature	Custom text automatically inserted at the end of each message.
ModWeb	Changes to this property are implemented immediately.
Identifier	Users associated with the current Parent object see this banner in the title bar of each WebAccess page.
Default Language	The default language for the Modular Web Agent and its sub-modules. This setting is implemented for users associated with the current Parent object.
Default Timezone	The default time zone for the Modular Web Agent and its sub-modules. This setting is implemented for users associated with the current Parent object.

Option	Function
Templates	NetMail WebAccess templates allow you to control the Modular Web Agent client interface. NetMail 3.5 ships with two client templates—WebAccess (Webacc.ctp) and Webmail (WebMail.ctp). The WebAccess interface provides standard mail client functionality, calendaring, scheduling, assigning tasks, and writing notes. Administrators can also use the WebAccess interface to delegate NetMail administrative functions such as adding, modifying, and deleting user accounts. (For more information on delegating NetMail administration, see “Task-Oriented Management” on page 262.) Webmail is patterned after the NIMS 2.5 mail client interface. It provides standard mail client functionality and administrators can use the Webmail interface to give users access to self-administration features like changing passwords and configuring vacation messages. For more information on templates, see “Calendar Agent” on page 99.
Default Template	The default mail client template for users associated with the current Parent object. Select the default template from the Available Templates list. **NOTE:** Users can select a different template in the mail client interface.
Available Templates	The templates that users associated with the current Parent object can select in the Modular Web client. To add templates to the list, 1. Click the browse button (...). 2. Click Add to browse the tree for Template objects. **NOTE:** To add a template to the list of available templates, you must first create a Template object in the Template container.
SMTP	Changes to this property are effective within 5 minutes.
Global Domains	The Global Domains associated with the current Parent object. You can associate Parent objects with both Global and Hosting Domains. **IMPORTANT:** Do not list a domain as both a Global Domain and a Hosting Domain. For the SMTP Agent to recognize Global Domains, you must include them in either the SMTP Agent's or the Parent object's Global Domains lists. For a complete discussion on how the messaging system uses Global Domains, see “Global Domains” on page 248. For an explanation of the SMTP Agent’s configuration options, see “Configuring the SMTP Agent” on page 90.

Option	Function
Hosting Domains	The Hosting Domains associated with the current Parent object. You can associate Parent objects with both Hosting and Global Domains. **IMPORTANT:** Do not list a domain as both a Global Domain and a Hosting Domain. For the SMTP Agent to recognize Global Domains, you must include them in either the SMTP Agent's or the Parent object's Global Domains lists. For a complete discussion on how the messaging system uses Hosting Domains, see "Hosting Domains" on page 250. For an explanation of the SMTP Agent's configuration options, see "Configuring the SMTP Agent" on page 90.
Relayed Domains (ETRN)	The current SMTP Agent services the ETRN Domains. To support these domains, you must click the Accept ETRN option in the Options page. For more information on ETRN Domains, see "Servicing ETRN Domains" on page 251.
Allowed Hosts	A list of IP ranges. If Require sender to be in "Allowed" list for remote sending is marked in the SMTP Agent, only the workstations that fall within the designated IP address ranges can relay messages through the SMTP server. This prevents users who are not members of the messaging system from using the SMTP Agent to relay messages over the Internet. Use this setting to prevent internal hosts from relaying Internet messages. To restrict which workstations that you allow to send remote messages, designate ranges of internal IP addresses. **NOTE:** If a workstation's IP address is not in an Allowed Hosts range, you can still use the workstation to send local messages (i.e., messages to other users in the messaging system).

Table 3 Template Object

Option	Function
Options	This object has no configurable options.

NetMail Agent Configuration Options

This section reviews the configuration options for each of the NetMail agents.

- Table 4, “Address Book Agent,” on page 360
- Table 3, “Alias Agent,” on page 362
- Table 3, “AntiSpam Agent,” on page 366
- Table 3, “AntiVirus Agent,” on page 367
- Table 3, “AutoReply Agent,” on page 369
- Table 3, “Calendar Agent,” on page 370
- Table 3, “Connection Manager,” on page 371
- Table 3, “IMAP Agent,” on page 371
- Table 3, “List Agent,” on page 371
- Table 3, “Modular Web Agent,” on page 372
- Table 3, “ModWeb Calendar Module,” on page 374
- Table 4, “ModWeb Mail Module,” on page 374
- Table 5, “ModWeb Preferences Module,” on page 376
- Table 6, “ModWeb Task Management Module,” on page 377
- Table 7, “NMAP Agent,” on page 377
- Table 3, “POP Agent,” on page 383
- Table 3, “Proxy Agent,” on page 383
- Table 3, “Rule Agent,” on page 384
- Table 3, “SMTP Agent,” on page 385

For an overview of agent functions, see “NetMail Agents” on page 8.

Table 4 Address Book Agent

Option	Function
Configuration	**IMPORTANT:** You must restart MSGLDAP to effect any changes in the Address Agent configuration. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)
Database Creation	How often (in days) the Address Book Agent recreates the address book index. The default is one day. The maximum setting is 99 days. To speed up LDAP queries, the Address Book Agent maintains an index of all the information queried for any user in its supported NMAP contexts—specifically, the users’ e-mail addresses, first names, last names, and full names. Although the index contains the user’s address book information, the Address Book Agent only uses the index to locate users in the tree. By default, all address book information, including the user’s e-mail address, is taken from the User object in NDS. This means the address book is always as current as NDS. **IMPORTANT:** ModWeb does not verify that the domain listed in the User Object’s Internet E-mail Address property is a supported Global or Hosting domain. Therefore, it is recommended you use the Alias Agent to populate this property or manually ensure the domain is valid.

Option	Function
Database Creation *continued*	If the user's e-mail address is not defined in the User object's Internet E-mail Address property, the Address Book Agent dynamically generates the e-mail address as follows: ◆ If the user belongs to a Hosting Domain, the Address Book Agent simply uses the username as the e-mail address. ◆ If the user belongs to a Global Domain, the Address Book Agent generates the e-mail address from the username and the user's Internet domain (username@domain). To identify the user's Internet domain, the Address Book Agent looks in the following objects: 1. If the user is associated with a Parent object, the Address Book Agent looks in the Parent object's Global Domains list. 2. If no Global Domain is configured in the Parent object, the agent looks for the user's Container Domain. 3. If no Container Domain is configured, the Address Book Agent uses the messaging server's Official Domain.
Port	Specifies the LDAP port assignment. LDAP applications (such as the Modular Web Client Address Book) access the Address Book Agent via this port for address book lookups. The Address Book Agent's default LDAP port assignment is 389, or on Novell Nterprise Linux Services, port 52389.
LDIF Export	Configures the Address Book Agent to automatically create an LDIF (LDAP Data Interchange Format) file of all user information, except information or accounts protected by User object privacy settings. Use this file to distribute address book information to messaging systems (such as remote sites) that do not have access to the Address Book Agent. The LDIF file is created as ADDRBOOK.LDF in the following directories: ◆ sys:\PUBLIC on NetWare systems ◆ \DBF\Shared on Windows systems ◆ /usr/lib on Linux systems The LDIF file is automatically regenerated every time the Address Book Agent updates its user index.
Allow Personal Addressbook Search	An LDAP search searches the user's personal address book if the LDAP connection is authenticated. For example, to authenticate the LDAP connection in Outlook Express*, the user must configure "My LDAP Server requires authentication" and type his or her NDS username and password.
Monitored Servers	Monitored servers are the NMAP Agents the Address Book Agent references to generate its index. Only those users belonging to contexts supported by the selected NMAP Agents are queried via the Address Book Agent. Conversely, User objects not included in a supported context are not included in the agent's index and, therefore, are not available for address book queries. Use the Browse button to locate and select one or more NMAP Agents.

Option	Function
Status	By default, the Address Book Agent is enabled. To disable the Address Book Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Address Book Agent at startup. However, to immediately disable the agent, you must manually unload MSGLDAP.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Address Book Agent is disabled, the messaging server does not launch MSGLDAP.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 Alias Agent

Option	Function
Configuration	**IMPORTANT:** You must restart MSGLDAP to effect any changes in the Alias Agent's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Database Creation	
Every _____ Day(s)	How often (in days) the Alias Agent regenerates the alias database. The default is 1 day. The maximum setting is 99 days. The alias database contains alias tables that store the aliases and their associated usernames. **NOTE:** 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 SNMP is configured).
Automatic Aliasing	If enabled, the Alias Agent automatically generates aliases for NDS User objects in the following formats: ◆ Firstname_Lastname@Domain (Steve_Johnston@novell.com) ◆ First Letter+Lastnam@Domain (Sjohnsto@novell.com) This alias option is limited to eight characters. ◆ Firstname.Lastname@Domain(Steve.Johnston@novell.com) ◆ Full.M.Name@Domain (Steve.W.Johnston@novell.com) ◆ Full_M_Name@Domain (Steve_W_Johnston@novell.com) The Fullname formats only work if the users' full names are provided in the Full Name field of their User objects. Automatically generated aliases are local aliases. Consequently, they are only recognized by the current Alias Agent. To ensure that these aliases are recognized throughout the messaging system, you can have only one Alias Agent.

Option	Function
Local Aliases	Aliases that are only recognized by the current Alias Agent. They are stored in the local Alias Agent's alias table. Local aliases are ideal when you are maintaining identical aliases, such as Admin or Webmaster, in a single messaging system. (See "Configuring Multiple User Objects Simultaneously" on page 208 for more information.) The following are the most common errors encountered with local aliases: ◆ The replacement string does not correspond to a valid username. ◆ The alias resolves to more than one user. ◆ The replacement string does not exactly match the username. ◆ The alias is not an exact match. ◆ If the user belongs to a Hosting Domain, the replacement string must match the user's full e-mail address (username@hostdomain). ◆ If the user does not belong to a Hosting Domain, the replacement string does *not* include the domain portion of the user's e-mail address.
Add	To create a local alias, 1. Type an alias in the left field. 2. Type the corresponding e-mail address (replacement string) in the right field. If the replacement string addresses a user in a Global Domain, type only the username. You cannot type the complete e-mail address because the domain portion of Global Domain e-mail addresses is stripped out by the SMTP Agent before the message enters the queue. For more information, see "Global Domains" on page 248. 3. Click Add. The alias appears in the list using the following syntax: *alias* string = *user_name* For example, if user SJohnsto wants users to send e-mail to SteveJ, the alias reads: `SteveJ = SJohnsto.` Then when users address e-mail to SteveJ, it is delivered to the SJohnsto mailbox. You could also create an alias such as feedback@company.com that would resolve to a local or remote e-mail address. 4. When you are finished providing aliases, click OK to save the aliases to the Alias Agent's local alias table.
Remove	To remove an alias, select the alias > click Remove.

Option	Function
Import	You can import local aliases in ASCII format if they use an *alias string =user_name* syntax with a carriage return and line feed (<CR><LF>) between lines. To import local aliases, 1. Click Import. 2. Browse to and select the ASCII file of aliases. 3. Click OK.
Global Aliases	Aliases that are recognized by every Alias Agent running on a distributed messaging server. Global aliases are stored in a shared alias table in the Internet Services container. The shared alias table includes entries from every Alias Agent running on a distributed messaging server. Other than the fact that global aliases are recognized throughout the messaging 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. **NOTE:** The preferred way to manage Global Aliases is to define NDS Alias objects. This is because NDS Alias objects provide all the functionality of Global Aliases, but they do not require an Alias Agent. (You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create Alias objects.)
Add	See Local Aliases.
Remove	See Local Aliases.
Import	See Local Aliases.
Queue Server	Queue Servers are the message queues monitored by the Alias Agent. Messages passing through the specified NMAP Agents' message queues are scanned by the Alias Agent. If a message recipient matches any of the Alias Agent's defined aliases, it replaces the alias with the corresponding e-mail address. A single Alias Agent can monitor multiple NMAP Agents' message queues. Use the Browse button to locate and select one or more NMAP Agents. **NOTE:** You cannot configure multiple Alias Agents to monitor the same NMAP Agent. Only one Alias Agent can monitor each NMAP server. To verify that an Alias Agent is registered to a particular NMAP Agent, view the Client property in the NMAP object. If registered, the server running the Alias Agent is listed as an NMAP client.

Option	Function
Monitored Queues	Monitored Queues are the NMAP Agent contexts for which the Alias Agent can automatically generate aliases. Use the Browse button to locate and select one or more NMAP Agents. When the Alias Agent generates automatic aliases, it references the Monitored Queues list. If a username exists within the selected NMAP Agents' contexts, the Alias Agent creates an alias. If the username does not exist within a supported context, no alias is created. To verify that an Alias Agent is registered to a particular NMAP Agent, view the Client property in the NMAP object. If registered, the server running the Alias Agent is listed as an NMAP client.
Status	By default, the Alias Agent is enabled. To disable the Alias Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Alias Agent at startup. However, to immediately disable the agent, you must manually unload MSGALIAS.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Alias Agent is disabled, the messaging server does not launch MSGALIAS.NLM again until you unmark Disable Agent and restart the messaging server.
Internet E-mail Address	
Automatic Attribute Population	
Automatically populate "Internet E-mail Address" attribute	Automatically populates the standard NDS attribute, Internet E-mail Address, with one of the following values: ◆ Default E-mail address For information on how the default e-mail address is derived, see "User E-mail Addresses" on page 195. ◆ Firstname_Lastname@Domain (Steve_Johnston@novell.com) ◆ First Letter+Lastnam@Domain (Sjohnsto@novell.com) This alias option is limited to eight characters. ◆ Firstname.Lastname@Domain(Steve.Johnston@novell.com) ◆ Full.M.Name@Domain (Steve.W.Johnston@novell.com) ◆ Full_M_Name@Domain (Steve_W_Johnston@novell.com) **NOTE:** The Fullname formats only work if the users' full names are typed in the Full Name field of their User objects.

Table 3 AntiSpam Agent

Option	Function
Configuration	**IMPORTANT:** You must restart ANTISPAM to effect any changes in the AntiSpam Agent's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Blocked Domains and Addresses	A blackout list of domains and e-mail addresses. Messages from these domains and e-mail addresses are removed from the designated message queues.
Add	To add a domain or e-mail address to the Blocked list, 1. Type a domain or e-mail address In the Blocked Sites box. For example *company.com* or Joe@*company.com*. If you type a domain name, all e-mail addresses ending with that domain are blocked. If you type a specific e-mail address, only that exact address is blocked. 2. Click Add.
Remove	To remove a domain or address from the Blocked list, 1. Select the domain or address. 2. Click Remove.
Import	You can import domains and e-mail addresses in ASCII format. You must separate each domain or e-mail address with a carriage return and line feed (<CR><LF>). To import domains and e-mail addresses, 1. Click Import. 2. Browse to and select the ASCII file of domains and e-mail addresses. 3. Click OK.
Send Back	Returns blocked messages to their senders with the message, "Mail from <*user or domain*> is blocked from this site."
CC Postmaster	Copies the postmaster on blocked messages that are returned to their senders. This option works in conjunction with Send Back.
Monitored Queues	A monitored queue is the message queue serviced by the AntiSpam Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AntiSpam Agent can monitor multiple message queues. Use the Browse button to select one or more monitored queues. **NOTE:** You cannot configure multiple AntiSpam Agents to monitor the same queue. Only one AntiSpam Agent can monitor each queue. To verify that an AntiSpam Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the AntiSpam Agent is listed as an NMAP client.

Option	Function
Status	By default, the AntiSpam Agent is enabled. To disable the AntiSpam Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the AntiSpam Agent at startup. However, to immediately disable the agent, you must manually unload ANTISPAM.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the AntiSpam Agent is disabled, the messaging server does not launch ANTISPAM.NLM again until you deselect Disable Agent option and restart the messaging server.

Table 3 **AntiVirus Agent**

Option	Function
AntiVirus Engine	**IMPORTANT:** You must restart AVIRUS to effect any changes in the AntiVirus Agent configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
CA InoculateIT	The AntiVirus Agent supports any Computer Associates InoculateIT-compliant virus engine. If properly configured, the NetMail AntiVirus Agent accesses the bare engine and performs all required scanning. Consequently, unless you also use the server for file and print services, Novell recommends that you do not run the full scanning engine. Allowing the AntiVirus Agent to perform all required scanning improves system performance because the agent does not scan the temporary and permanent files written by NetMail. If you need to run the full scanning product, you must first load InoculateIT in the AUTOEXEC.NCF file before loading NetMail; InoculateIT cannot start if its engine (AVENGINE.NLM) is already loaded. In this configuration, you must also ensure that you never unload InoculateIT without first unloading the NetMail AntiVirus Agent.
McAfee	The AntiVirus Agent supports any McAfee NetShield-compliant virus engine. If properly configured, the NetMail AntiVirus Agent accesses the bare engine and performs all required scanning. Consequently, unless you also use the server for file and print services, Novell recommends that you do not run the full scanning engine. Allowing the AntiVirus Agent to perform all required scanning improves system performance because the agent does not scan the temporary and permanent files written by NetMail.

Option	Function
Pattern-file path:	The path to the virus engine's pattern file. **IMPORTANT:** Do not include the filename. The pattern file is a virus definition file that you download periodically from the McAfee of Computer Associates web site to keep your virus protection up to date.
Symantec CarrierScan Server	The AntiVirus Agent supports any Symantec CarrierScan-compliant engine. The Symantec CarrierScan server is the server running the virus engine.
Host	The hostname or IP address of the server running the Symantec CarrierScan engine.
Port	The port at which the AntiVirus Agent can connect to the CarrierScan engine.
Scanning	The scanning options determine which messages are scanned for viruses.
Only scan messages for local recipients	Only scans messages addressed to users for whom virus scanning is enabled. You can enable virus scanning at the Parent or User objects.
Scan all messages	Scans all messages that pass through the AntiVirus Agent's monitored queues.
Behavior	
Notify intended recipient if infected	Sends a virus alert to the message recipient(s). The alert indicates who tried to send the message and which virus the message contained.
Return to sender if infected	Returns the message to the sender with a notice indicating which virus the message contained.
Monitored Queues	A monitored queue is the message queue serviced by the AntiVirus Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AntiVirus Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. To verify that an AntiVirus Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the AntiVirus Agent is listed as an NMAP client.

Option	Function
Status	By default, the AntiVirus Agent is enabled. To disable the AntiVirus Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the AntiVirus Agent at startup. However, to immediately disable the agent, you must manually unload AVIRUS.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.
Status *continued*	After the AntiVirus Agent is disabled, the messaging server does not launch AVIRUS.NLM again until you deselect the Disable Agent option and restart the messaging server. **NOTE:** When you initially unload AVIRUS.NLM, the messaging system is not left unprotected. Due to the design of the message queue, NMAP temporarily pauses message processing while it tries to connect to the AntiVirus Agent. It attempts a connection several times before it continues message processing without the agent. This timeout period (approximately 30 seconds) provides enough time to reload the AntiVirus Agent after updating pattern files or engine code. If you are using the InoculateIT engine without running the full scanning product, you only need to update the pattern file and/or the engine NLM. NetMail automatically detects any such update, pauses the queue, reloads the engine and the new pattern files, and then resumes message processing.

Table 3 **AutoReply Agent**

Option	Function
Monitored Queues	A monitored queue is the message queue serviced by the AutoReply Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single AutoReply Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. **NOTE:** You cannot configure multiple AutoReply Agents to monitor the same queue. Only one AutoReply Agent can monitor each queue. To verify that an AutoReply Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the AutoReply Agent is listed as an NMAP client. **IMPORTANT:** You must restart FORWARD to effect any changes in the Monitored Queues configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option	Function
Status	By default, the AutoReply Agent is enabled. To disable the AutoReply Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the AutoReply Agent at startup. However, to immediately disable the agent, you must manually unload FORWARD.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the AutoReply Agent is disabled, the messaging server does not launch FORWARD.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 Calendar Agent

Option	Function
Monitored Queues	A monitored queue is the message queue serviced by the Calendar Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single Calendar Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. **NOTE:** You cannot configure multiple Calendar Agents to monitor the same queue. Only one Calendar Agent can monitor each queue. To verify that an Calendar Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the Calendar Agent is listed as an NMAP client. **IMPORTANT:** You must restart CALAGENT to effect any changes in the Monitored Queues configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Status	By default, the Calendar Agent is enabled. To disable the Calendar Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Calendar Agent at startup. However, to immediately disable the agent , you must manually unload CALAGENT.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Calendar Agent is disabled, the messaging server does not launch CALAGENT.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 Connection Manager

Option	Function
Configuration	
Expire Addresses after _____ minutes	The amount of time (in minutes) that an IP address is stored by the Connection Manager Agent. You can designate any value between 5 and 1440 minutes. **IMPORTANT:** You must restart GKEEPER to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Status	By default, the Connection Manager Agent is enabled. To disable the Connection Manager Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Connection Manager Agent at startup. However, to immediately disable the agent, you must manually unload GKEEPER.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the Connection Manager Agent is disabled, the messaging server does not launch GKEEPER.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 IMAP Agent

Option	Function
Status	By default, the IMAP Agent is enabled. To disable the IMAP Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the IMAP Agent at startup. However, to immediately disable the agent, you must manually unload IMAPD.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the IMAP Agent is disabled, the messaging server does not launch IMAPD.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 List Agent

Option	Function
Configuration	**IMPORTANT:** You must restart IMSLIST to effect any changes in the List Agent configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option	Function
Create Digests Daily At _____ hours	The time each day when the List Agent compiles and distributes Mailing List digests. Specify the time using the 24-hour clock. A digest is a compilation of the messages broadcast over a mailing list in a 24-hour period. The List Agent only generates digests for Mailing List objects that have the Generate Digest option selected in the mailing list configuration menu.
Monitored Queues	A monitored queue is the message queue the List Agent monitors for messages addressed to mailing lists. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single List Agent can monitor multiple message queues. Use the Browse button to select one or more monitored queues. **NOTE:** You cannot configure multiple List Agents to monitor the same queue. Only one List Agent can monitor each queue. To verify that a List Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the List Agent is listed as an NMAP client.
Status	By default, the List Agent is enabled. To disable the List Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the List Agent at startup. However, to immediately disable the agent, you must manually unload IMSLIST.NLM or restart the messaging server. For more information about manually unloading NetMail agents or restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317. After the List Agent is disabled, the messaging server does not launch IMSLIST.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 **Modular Web Agent**

Option	Function
Configuration	**IMPORTANT:** You must restart MODWEBD to effect any changes in the Modular Web Agent’s configuration. See “Loading and Unloading NetMail Agents” on page 317 for more information.
Ports	

Option	Function
HTTP Port	The port the Modular Web Agent uses for HTTP connections. The default HTTP port assignment is port 80 or, on Novell Nterprise Linux Services, port 52080. Use the default port number unless that port number is already in use by another program on the server. **IMPORTANT:** The NetWare® Management Portal also uses the default HTTP port assignment of 80. If you are running the NetWare Management Portal NLM on your messaging server (HTTPSTK.NLM), users are not able to reach the Modular Web Agent. For users to reach the Modular Web Agent, you must unload HTTPSTK.NLM from your Modular Web Agent server, change the NetWare Management Portal's port assignment, or change the Modular Web Agent's port assignment. Otherwise, when users type the Modular Web Agent server's IP address or hostname, they launch the NetWare Management Portal.
HTTPS (SSL) Port	The port the Modular Web Agent uses for secure HTTP (HTTPS) connections. The default HTTPS port assignment is port 443 or, on Novell Nterprise Linux Services, port 52443. Use the default port number unless that port number is already in use by another program on the server.
Identifier	The name of your company. This appears in the title bar of each client window.
Templates	NetMail templates allow you to control the mail client interface. NetMail 3.5 ships with two client templates—WebAccess and Webmail. The WebAccess interface provides standard mail client functionality, calendaring, assigning tasks, and writing notes. Administrators can also use the WebAccess interface to delegate NetMail administrative functions such as adding, modifying, and deleting user accounts. Webmail is the NIMS 2.5 mail client interface. It provides standard mail client functionality and administrators can use the Webmail interface to give users access to self-administration features like changing passwords and configuring vacation messages. For more information, see "Configuring the Calendar Agent" on page 100.
Default Template	The template NetMail uses if no template is defined in the User and Parent objects. Select the default template from the Available Templates list.
Available Templates	The list of available templates. To add templates to the list, 1. Click the Browse button (...). 2. Click Add to browse for additional templates. **NOTE:** To add a template to the list of available templates, you must first create the template object in the Template container.
Default Timezone	The default time zone for the Modular Web Agent and its sub-modules. The time zone defined in the Parent object, User object, or User Preferences overrides this default setting.

Option	Function
Default Language	The default language for the Modular Web Agent and its sub-modules. The language defined in the Parent object or User Preferences overrides this default setting.
Status	By default, the Modular Web Agent and its plug-in modules are enabled. To disable the Modular Web Agent and its plug-ins, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Modular Web Agent and its plug-in modules at startup. However, to immediately disable the agent and its plug-in modules, you must manually unload MODWEBD.NLM or restart the messaging server. For more information about manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.) After the Modular Web Agent is disabled, the messaging server does not launch MODWEBD.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 **ModWeb Calendar Module**

Option	Function
Queue Server	The queue server is the NMAP Agent to which the ModWeb Calendar Module delivers appointments, notes, and tasks that the message queue needs to process. Each ModWeb Calendar Module can have only one queue server. Use the Browse button to select any NMAP Agent in the tree. If the ModWeb Calendar Module and NMAP Agent are not running on the same server, you can make the server running the ModWeb Calendar Module a trusted host of the NMAP Agent for faster server access. For more information, see the Trusted Hosts property in Table 4, "Configuring the NMAP Agent," on page 68. To verify that the ModWeb Calendar Module is registered to a particular queue server, view the Client property in the NMAP object. If registered, the server running the ModWeb Calendar Module is listed as an NMAP client. **IMPORTANT:** You must restart MODWEBD to effect any changes in the ModWeb Calendar Module's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Table 4 **ModWeb Mail Module**

Option	Function
Configuration	**IMPORTANT:** You must restart MODWEBD to effect any changes in the ModWeb Mail Module's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Limits	

Option	Function
Message Size Limit	The maximum message size users can send from the Modular Web Agent. The ModWeb Mail Module does not restrict the size of inbound messages the Modular Web Agent downloads from the user's mailbox.
Maximum number of recipients per mail	Limits the number of recipients per message sent by users from the Modular Web Agent client. The ModWeb Mail Module does not restrict the number of recipients for inbound messages that the Modular Web Agent client downloads from the user's mailbox.
Addressbook	The Addressbook options allow you to control which address books users can access from the Modular Web mail templates. **NOTE:** To sort the ModWeb address books, see "Configuring the Mail Module" on page 86.
Personal	Allows Modular Web Agent users to create personal address books. Users' personal address books are stored in their NDS User object. Consequently, users can access their personal address book from any location as long as they are logged in to the network.
System-Wide	If marked, this option gives users access to a system-wide address book in the Modular Web client (WebAccess or Webmail). In the LDAP URL field, you can type the following LDAP parameters: ldap://user:password@hostname:port/?basedn ◆ The *user:password* variable is the user's name and password. ◆ *Hostname* identifies the LDAP server's host name or IP address. If you type the IP address of a server running the Address Book Agent, users can access address book information from eDirectory. ◆ *Port* specifies the LDAP port assignment. If the LDAP server uses the default LDAP port (port 389), you do not need to specify a port. ◆ *Basedn* identifies the address book context. This is required if the Require DN attribute is added to the Address Book Agent. It is ignored if the Derive DN from Authentication is added to the Address Book Agent. (See "Address Book Agent Optional Features" on page 110 for more information.) Users with the Privacy attribute set to Limited or None in their NDS User object are visible to other NetMail users in the System-Wide Addressbook. Users with an listed privacy setting are not visible in the System-Wide Addressbook. **NOTE:** For information on providing domain-specific address books, see "Managing Multiple Address Books" on page 258.
Public	If marked, this option allows users to define their own public address books in the Modular Web client (WebAccess or Webmail). To define a default Public LDAP Server, type the host name or IP address of any public LDAP server in the LDAP URL field. You can use the same LDAP parameters discussed under System-Wide LDAP Server.

Option	Function
Queue Server	The queue server is the NMAP Agent to which the ModWeb Mail Module delivers messages that the message queue needs to process. Each ModWeb Mail Module can only have one queue server. Use the Browse button to select any NMAP Agent in the tree. If the ModWeb Mail Module and NMAP Agent are not running on the same server, you can make the server running the ModWeb Mail Module a trusted host of the NMAP Agent to expedite server access. For more information, see the Trusted Hosts property in Table 4, “Configuring the NMAP Agent,” on page 68. To verify that the ModWeb Mail Module is registered to a particular queue server, view the Client property in the NMAP object. If registered, the server running the ModWeb Mail Module is listed as an NMAP client.

Table 5 ModWeb Preferences Module

Option	Function
Configuration	**IMPORTANT:** You must restart MODWEBD to effect any changes in the Preference Module’s configuration. See “Loading and Unloading NetMail Agents” on page 317 for more information.
Passwords	
Allow Users to Change Password	Enables users to change their login password from the Modular Web Agent templates. Because NetMail is completely integrated with NDS, the user’s ModWeb password is the same as the user’s NetWare login password. Therefore, marking this option actually gives your users rights to their NetWare login password through Modular Web Agent, regardless of whether they have rights to the actual password property in their NDS User object.
SSL Required	Requires Modular Web Agent users to make an SSL connection to the server running the ModWeb Preferences Module before they can change their passwords. **NOTE:** You must have a server certificate installed on the current messaging server before you can enable this option. For information on setting up your server certificate, see “Setting Up TLS and SSL” on page 231.
Disable Options	Disables user configuration options in the WebAccess and Webmail templates. If marked, these options do NOT appear in the User Preferences menu.
Timeout	The amount of idle time before the user is automatically logged out of the Modular Web client.
Colors	Template color definition options. This option is specific to the Webmail template.
Signature	Custom text automatically inserted at the end of each message.
Privacy	The user’s level of privacy within the messaging system. The privacy level controls what the Address Book Agent reveals about the user.

Table 6 ModWeb Task Management Module

Option	Function
Information	This Task Oriented Management Module has no configurable options. However, you must run it on the messaging server to enable TOM administration. See "Task-Oriented Management" on page 196 for more information on configuring TOM administration.

Table 7 NMAP Agent

Option	Function
Parameters	
Storage Paths	**IMPORTANT:** You must restart NMAPD to effect any changes in these properties. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Message Store	The volume and, optionally, the directory where users' mailboxes are located. On a NetWare server, the message store's default location is sys:\NOVONYX\MAIL. On a Windows server, the default message store directory is \Program Files\novell\netmail\mail. On a Linux server, the default location is the /usr/nims directory. For detailed information about the message store directory structure, see "Message Store Directory Structure" on page 19. **IMPORTANT:** Because NetWare requires free space on the sys: volume, 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, 1. Stop the NMAP Agent. 2. Move the existing message store directory to its new location. 3. Change the location specified in the NMAP Agent's Message Store field. 4. Restart the NMAP Agent. (See "Loading and Unloading NetMail Agents" on page 317.) **IMPORTANT:** It is best to change the message store volume before you put your NetMail system into production. In addition to the primary message store on the messaging server, you can define message store directories for Container and Parent objects. For more information, see "Creating Separate Message Stores for Each Domain" on page 260.
Spool Directory	The volume and, optionally, the directory where you want the message queue to reside. For detailed information about the Spool directory structure and how the message queue works, see "Message Processing" on page 19.

Option	Function
Minimum Space	The minimum amount of free space you want to maintain on the volume hosting the message queue. The default is 2048 KB. If the server reaches the Minimum Space quota, the messaging server bounces all incoming messages, stops system logging, and sends an SNMP trap. If your mail directories are on the sys: volume, you can use this option to maintain the free space required by NetWare.
SCMS Directory	The volume and, optionally, the directory where you want the Single Copy Message Store (SCMS) directory to reside. For detailed information about the SCMS directory structure and how it works, see "Single Copy Message Store" on page 20.
Queue Parameters	
Retry Interval	The number of minutes the NMAP Agent waits before trying to resend any e-mail message. The default is 30 minutes. NetMail never queues messages unless there is a problem. Under normal conditions, the NMAP Agent immediately tries to send messages after they are processed in the queue. If, for some reason, the message is not sent, it remains in the queue for the number of minutes specified in the Retry Interval before NMAP tries to resend the message. For example, if you send a message to a company whose mail server is down, the messaging server keeps trying to send the message at the designated intervals. Changes to this property are effective within 5 minutes.
Retry Timeout	The number of days the NMAP Agent keeps trying to send any e-mail message before removing the message from the queue. The default is five days. The NMAP Agent attempts to bounce undeliverable messages before removing them. **IMPORTANT:** You must restart NMAPD to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Options	
Bounced Message Control	A UBE control feature that sets a threshold for the number of bounced messages NMAP can process within a set number of seconds. If the number of bounced messages exceeds the defined threshold, the messages are deleted instead of processed. It is a common practice for spammers to falsify the From: field in their message so the resulting bounced messages go to a mail server other than their own. Unfortunately, the server that actually owns the domain specified in the From: field is inundated with thousands of bounced messages in a short period of time. The Bounced Message Control feature enables you to keep your NetMail system from wasting system resources during such attacks. Changes to this property are effective within 5 minutes.

Option	Function
CC Postmaster	Mark this option to send the Postmaster a copy of bounced messages.
Limit Bounces To	Select this option to turn on Bounced Message Control. ◆ **Interval**: The time frame threshold (in seconds). ◆ **Entries**: The number of bounced messages NMAP can process during the *Interval* time frame. If the number of bounced messaged exceed the *Entries* threshold within the *Interval* timeframe, NMAP deletes the messages.
Forward Local Undeliverable Messages	The host name or IP address of a server designated to receive messages that are addressed to the messaging system's domain but are undeliverable within the local NetMail 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 e-mail address. Changes to this property are effective within 5 minutes. 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 re-queues the message. WAN environments commonly use this feature with standalone messaging servers in remote offices. For detailed information on this configuration, see "Multiple Messaging Server WAN" on page 36.
Forward Local Undeliverable Messages *continued*	This option also enables NetMail to share a domain name with another e-mail system such as Novell GroupWise®, Lotus Notes*, or Microsoft* Exchange. When this option is configured, the NMAP Agent forwards messages that belong to the domain but are not addressed to users within the NetMail messaging system. For more information on domain sharing, see "Domain Sharing" on page 251.
Remote Queue Restrictions	Regulates when remote messages are passed to the SMTP Agent for delivery across the Internet. If Do not process remote queue is selected, NMAP holds remote messages in queue 7 until the designated time frames. Only then does it notify the SMTP Agent to pick up the messages. In the Weekdays field, specify a time span (using the 24-hour clock) when you do not want the NMAP Agent to process outgoing messages Monday through Friday. In the Weekends field, do the same for Saturday and Sunday. This feature is for countries where users must pay a per use line fee. Using this option, you can restrict remote message delivery to non-peak hours. **IMPORTANT:** You must restart NMAPD to effect any changes in this property. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)

Option	Function
Context	The NDS contexts serviced by the current NMAP Agent. The original context was defined when creating the NMAP Agent. Add other user contexts from the Context page. Because NMAP contexts are not inherited, add every container or sub-container serviced by an NMAP Agent to that agent's context list. Messaging services are automatically provided to every user in the NMAP Agent's assigned contexts. User mailboxes are created in the local message store directory the first time users log in or receive messages. **IMPORTANT:** Do not add the same context to multiple NMAP Agents.This produces unpredictable behavior in NetMail systems. In previous NetMail versions, the messaging server's context list was not updated in memory. Consequently, if you added or removed contexts in the NMAP Agent configuration, the changes did not take effect until the messaging server was restarted. In NetMail 3.5, however, the messaging server's context list is updated in memory; therefore, it is no longer necessary to restart the messaging server. The Messaging Server's Context List NMAP contexts are tracked by the messaging server. When it starts, the messaging server generates a list of NMAP contexts and holds it in server memory. In distributed environments, the context list includes the assigned contexts for every NMAP Agent in the Internet Services container. On standalone messaging servers, this list only includes the local NMAP Agent's assigned contexts. NetMail agents reference the messaging server's context list in providing user-related services. If a user is not included in the list, the agent's services are denied. For example, users cannot establish a POP or IMAP connection to the messaging system unless they are in the context list. System Requirements NDS requires a minimum of 3 KB per User object replicated on the server. Therefore, in addition to the standard NetMail disk space requirements, you must calculate at least an additional 3 KB for every NDS User object in the NMAP Agent's context. Additionally, the NMAP Agent requires local access to all User objects within its assigned contexts.
Mailbox Quota	The system administrator can define mailbox quotas for specific users or for all users serviced by the current NMAP Agent. Messages, folders, and calendar items count against the mailbox quota. **IMPORTANT:** You must restart NMAPD to effect any changes in these properties. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Per User Mailbox Quotas	Mark this option to require individual user quotas. User quotas are set in the NetMail Configuration page of the User object. For further information on User object configuration, see Table 5, "User Objects," on page 394.

Option	Function
System-Wide Mailbox Quotas	To set the same quota for all mailboxes on the current messaging server, mark this option and type the maximum mailbox size in the Kbyte field. If you select both Per User and System-Wide Mailbox Quotas, you can set quotas at both levels. While the system-wide quota serves as the default quota for all users in the NMAP Agent's assigned contexts, quotas defined in the User object take precedence. For example, you can set a default, system-wide mailbox quota but still allocate more disk space to specific users such as the messaging server postmaster, system administrators, or VIPs using User object mailbox quotas. **NOTE:** You can also define mailbox quotas at the Parent object level. For more information on Parent object mailbox quotas, see the Mailbox Quota property in Table 3, "Configuring Parent Objects," on page 262.
Quota Return Message	An optional message that is returned to the sender when the recipient has exceeded his or her mailbox quota. The message notifies the sender that the recipient has exceeded the allotted mailbox quota and cannot receive additional messages. **NOTE:** When users are within 10% of their mailbox quota, they receive a system message notifying them that their mailbox is almost full. The message advises them to delete some of the messages and warns that when their mailbox is full, all inbound messages are returned to the sender.
Single Copy Message Store	The Single Copy Message Store (SCMS) feature allows NMAP to store e-mail messages sent to multiple recipients in a shared location on the messaging server. By default, messages sent to five or more users and exceeding 5 KB are stored in the shared message directory. To store a message in the SCMS directory, it must exceed both thresholds. When a message exceeds the specified thresholds, NMAP places a single copy of the message and its attachments in the shared message directory. A pointer is placed in the recipients' mailboxes, directing NMAP to the complete message in the Single-Copy Message Store (SCMS) directory. When the last user downloads or deletes the message, it is deleted from the shared directory. The SCMS feature conserves server disk space. Without SCMS, long messages and large attachments are sent to every recipient's mailbox, rapidly consuming large amounts of server disk space. Changes to this property are effective within 5 minutes. For more information on the SCMS directory, see "Single Copy Message Store Directory Structure" on page 21.
Minimum Number of Recipients	The SCMS threshold for a message's number of recipients. If the number of message recipients is equal to or more than the designated number of recipients and it exceeds the Minimum Message Size threshold, it is stored in the SCMS directory.
Minimum Message Size	The SCMS threshold for a message's minimum size, in kilobytes. If a message is larger than the designated message size and it exceeds the Minimum Number of Recipients threshold, it is stored in the SCMS directory.

Option	Function
Status	By default, the NMAP Agent is enabled. To disable the NMAP Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the NMAP Agent at startup. However, to immediately disable the agent, you must manually unload NMAPD.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the NMAP Agent is disabled, the messaging server does not launch NMAPD.NLM again until you deselect the Disable Agent option and restart the messaging server.
Trusted Hosts	When NetMail agents need to access the message store or message queue, they create an IP connection to the associated NMAP Server and request the information they need. By default, the NMAP Agent requires all agents running on other servers (including other NMAP Agents) to authenticate with the server before it carries out their requests. **NOTE:** NetMail agent authentication does not use clear-text passwords. By designating a messaging server as a trusted host, agents running on that server are not required to authenticate with the NMAP server. Rather, they are given open access to the NMAP Agent and its accompanying message queues and mail directories. Although not required, designating trusted hosts improves performance in distributed messaging systems. Changes to this property are effective within 5 minutes. **IMPORTANT:** Because trusted hosts have complete access to all mailboxes and queued messages, ensure that messaging servers with trusted host status are secure. Additionally, do not grand trusted host status to Linux machines unless login access to the trusted host machines is restricted to the system administrator.
Trusted Clients of this NMAP Server	
Add	To add a trusted host, 1. Type the IP address of a messaging server hosting NetMail agents that need open access to the NMAP Agent. 2. Click Add. On NetWare, because 127.0.0.0 and localhost are automatically trusted hosts, you do not need to add them to the list.
Remove	To remove a trusted host, select the trusted host > click Remove.
Clients	This page lists all NetMail agents that are registered to the current NMAP Agent. Agents that are typically clients of the NMAP Agent are the POP, IMAP, Modular Web Agent, etc., regardless of whether they reside on the current messaging server or on a remote messaging server. This is an informational page; you cannot add agents to or delete agents from the list.

Table 3 POP Agent

Option	Function
Status	By default, the POP Agent is enabled. To disable the POP Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the POP Agent at startup. However, to immediately disable the agent, you must manually unload POP3D.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317. After the POP Agent is disabled, the messaging server does not launch POP3D.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 Proxy Agent

Option	Function
Configuration	**IMPORTANT:** You must restart MAILPROX to effect any changes in the Proxy Agent's configuration. (See "Loading and Unloading NetMail Agents" on page 317 for more information.)
Run pickup every ___ hours	The number of hours that elapse between each message retrieval cycle.
Pickup Threads	The number of threads you want to use to simultaneously retrieve messages. The more threads, the faster the message retrieval, but additional threads consume additional server memory.
Monitored Servers	Monitored Servers are the messaging system contexts serviced by the Proxy Agent. Because NMAP Agents determine the messaging system's contexts, Monitored Servers correspond to NMAP Agents. Users belonging to contexts supported by the selected NMAP Agents can proxy other mail accounts. Use the Browse button to locate and select one or more NMAP Agents.
Queue Server	The queue server is the NMAP Agent to which the Proxy Agent delivers messages that the message queue needs to process. Each Proxy Agent can only have one queue server. Use the Browse button to select any NMAP Agent in the tree. If the Proxy and NMAP Agents are not running on the same server, you can make the server running the Proxy Agent a trusted host of the NMAP Agent to expedite server access. For more information, see the Trusted Hosts property in Table 4, "Configuring the NMAP Agent," on page 68. To verify that a Proxy Agent is registered to a particular queue server, view the Client property in the NMAP object. If registered, the server running the Proxy Agent is listed as an NMAP client.

Option	Function
Status	By default, the Proxy Agent is enabled. To disable the Proxy Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Proxy Agent at startup. However, to immediately disable the agent, you must manually unload MAILPROX.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317. After the Proxy Agent is disabled, the messaging server does not launch MAILPROX.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 Rule Agent

Option	Function
Monitored Queues	A monitored queue is the message queue serviced by the Rule Agent. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single Rule Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. **NOTE:** You cannot configure multiple Rule Agents to monitor the same queue. Only one Rule Agent can monitor each queue. To verify that a Rule Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the Rule Agent is listed as an NMAP client. **IMPORTANT:** You must restart RULESRV to effect any changes in the Monitored Queues configuration. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)
Status	By default, the Rule Agent is enabled. To disable the Rule Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the Rule Agent at startup. However, to immediately disable the agent, you must manually unload RULES.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317. After the Rule Agent is disabled, the messaging server does not launch RULES.NLM again until you deselect the Disable Agent option and restart the messaging server.

Table 3 SMTP Agent

Option	Function
Identification	You must add all the domain and host names that your NetMail system is planning to accept messages in either the Global or Hosting Domains list. In listing the domains that belong to your messaging system, consider the following important points: ◆ Do not list a domain as both a Global Domain and a Hosting Domain. ◆ Failure to add all domain and host names that resolve to the server's IP address creates message loops that quickly consume all your server resources. The problem is that messages addressed to domains not included in the SMTP Agent's domain lists still resolve to the SMTP server's IP address. However, because they aren't listed in the domain lists, the SMTP Agent cannot accept them. Therefore, the SMTP server ends up relaying these messages to itself in an endless loop. (NetMail only prevents such loops for domains that resolve to loopback or the server's default IP address.)
Global Domains	A listing of the messaging system's native domains. When the SMTP Agent receives a message, it looks at the domain portion of the recipient's e-mail address (everything after the @ symbol). If the addressed domain matches a domain in the Global Domains list, the SMTP Agent removes the domain portion of the address and drops the message in the message queue. Because the SMTP Agent removes Global Domains from the recipient's e-mail address, ensure that the user portion of the e-mail address (everything before the @ symbol) is unique. You can address unique usernames at any global domain. For example, messages addressed to Bob@Novell.com and Bob@Novell.edu are delivered to the same mailbox if Novell.com and Novell.edu are listed as Global Domains and an NDS object named Bob exists in an NMAP Agent context. (For more information on NMAP Agent contexts, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68.) **IMPORTANT:** In NetMail 3.5, you do *not* need to restart the SMTP Agent after adding domains to the Global Domains list. New domains are recognized by the SMTP Agent within 5 minutes.

Option	Function
Identification *continued*	
Hosting Domains	A listing of foreign domains hosted on the current system. This option is most applicable to ISP environments. For more information, see "Hosting Domains" on page 250. When the SMTP Agent receives a message addressed to a domain in the Hosting Domains list, it drops the message in the message queue *without* removing the domain portion of the recipient's e-mail address. Because the entire e-mail address remains intact, it is not necessary that the user portion of the e-mail address (everything before the @ symbol) is unique. Combining the user's name with a Hosting Domain name enables identical users to exist within the same messaging system. Although, you might have multiple users named "jling" in your overall messaging system, each one has a unique NDS username. **NOTE:** Because the user's e-mail address is also the user's NDS username, the user must type his or her full e-mail address (*username*@*domain*) to log in to the system. In NetWare Administrator, to create User objects that include the username and domain name, the period in the domain name must be escaped. For example, the user jling@hostdomain.com is created and displayed as jling@hostdomain\.com. Users created with domains in their NDS object names can only be addressed at that domain. For example, messages addressed to Bob@Novell.com and Bob@Novell.edu are delivered to different mailboxes if Novell.com and Novell.edu are listed as Hosting Domains and NDS objects named Bob@Novell.com and Bob@Novell.edu exist in an NMAP Agent context. (For more information on NMAP contexts, see the Context property in Table 4, "Configuring the NMAP Agent," on page 68) **NOTE:** In POP mode, Netscape* Messenger 4.x strips @ symbols and trailing characters from usernames. Users in Hosting Domains can use either Netscape Messenger 4.x in IMAP mode or they can manually configure a POP client to accept usernames with the @ symbol.
Hosting Domains *continued*	In NetMail 3.5, you do *not* need to restart the SMTP Agent after adding domains to the Hosting Domains list. New domains are recognized by the SMTP Agent within 5 minutes. **NOTE:** To enable the Netscape Messenger* 4.*x* POP client to accept usernames with the @ symbol, edit the PREFS.JS file in the C:\PROGRAM FILES\NETSCAPE\USERS*USERNAME* directory. Add the following line above the other mail lines: user_pref("mail.allow_at_sign_in_user_name", true) You can then restart the Netscape Messenger 4.*x* POP client. It is possible to make this change before distributing the Netscape client to all the users.
Limits	

Option	Function
Message Size Limit	The maximum message size the SMTP Agent can accept. Because the SMTP Agent handles all Internet traffic, this property limits both incoming and outgoing Internet messages. You can type any amount between None (no limit) and 40 MB. Changes to this property are implemented within 5 minutes.
Options	
Flags	A series of standard SMTP commands that you can enable on the current SMTP Agent. Select the commands you want the SMTP Agent to accept. Changes to the STMP flags are implemented within 5 minutes.
Allow Clients to Use VRFY Command	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 usernames. For example, if spammers want to find out the usernames in your company, they could query the system with a series of usernames until the system verified a valid username. When verifying that a user exists in the messaging system, the SMTP Agent references the context list maintained by the messaging server. If the user is not listed in the context list, the SMTP Agent returns a "User Not Found" message. See the Context property in Table 4, "Configuring the NMAP Agent," on page 68. for more information on the NMAP Agent's context list.
Options *continued*	
Allow Clients to Use EXPN Command	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 makes a request to expand a system-wide group such as Everyone, the SMTP Agent returns the complete membership list, which is, essentially, every username in your organization.
Verify Recipient Addresses When Accepting Messages	By default, the SMTP Agent accepts all incoming messages and places them in a queue where their addresses are verified, as resources are available. This process facilitates rapid message processing. However, if you want the SMTP Agent to perform address verification before accepting messages into your NetMail system, select Verify Addresses on Receipt. **IMPORTANT:** NetMail Aliasing does not work if Verify Recipient Addresses When Accepting Messages is selected. When this option is enabled, the SMTP Agent intercepts messages before they are processed in the message queue; consequently, messages addressed to NetMail aliases are deleted before the Alias Agent can process them. For more information on the Alias Agent, see "Managing User Aliases" on page 253.
Send ETRN to Servers	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. For more information, see "Servicing ETRN Domains" on page 251.

Option	Function
Accept ETRN from Clients	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. For more information, see “Servicing ETRN Domains” on page 251.
Mail Relay Host [Forwarder]	A mail relay host is a relay point for remote messages. It is often used to transfer outbound messages through a firewall. ETRN Domains also use Mail Relay Hosts to transfer messages to their relay service. (See “Servicing ETRN Domains” on page 251 for more information.) **IMPORTANT:** You must restart SMTPD to effect any changes in the Mail Relay Host configuration. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)
Use Relay Host	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 you plan to use as the mail relay host. All remote messages going through this SMTP Agent are then forwarded to the SMTP Agent at the designated address.
UBE Blocking	This page provides options that block incoming messages from specified sites. These options are designed to protect your messaging system from unsolicited bulk e-mail (UBE) or SPAM. Changes to these properties are implemented within 5 minutes.
Flags	
Do Not Allow Access from Hosts in Blocked List	Restricts access to your messaging system. If selected, the SMTP Agent refuses connections from any mail host with an IP address designated in the Blocked Hosts list.
Deny Access to Hosts Not in DNS	Provides reverse DNS lookups. When receiving messages from external systems, the SMTP Agent verifies that the host’s IP address and domain correspond to its DNS record. If they don’t match, the SMTP Agent drops the connection. **NOTE:** You must configure your DNS server to support reverse DNS lookups for this option to function.
Override with Authentication	This option provides an exception to the Deny Access to Hosts Not in DNS option. If marked, hosts that are not listed in DNS are given the opportunity to authenticate with the SMTP Agent before their connection is dropped.
RBL Check	Enables the SMTP Agent to do lookups on the Realtime Blackhole List (RBL*). RBL maintains a list of confirmed spammers and open relays. If the mail host matches an entry on the RBL, the connection is refused. To enable this option, mark Perform Check.

Option	Function
Add	To add an RBL site, type the IP address or host name of the RBL list server and click Add. The RBL entry can include a trailing semi-colon (;) and subsequent text. The text following the semi-colon is displayed as part of the protocol reply informing the sender he is blocked. The following configuration entry references bl.spamcop.net as the RBL Host and then adds a message directing the sender to the SpamCop web site. bl.spamcop.net;You have been blackholed by spamcop.net. Please see http://spamcop.net to get removed If the character sequence *%d.%d.%d.%d* is provided as part of the text, it is replaced by the IP address of the blocked system. Use this feature to generate responses containing URLs that point directly to the RBL system's look-up page. For example, in this configuration entry, bl.spamcop.net;Please see http://spamcop.net/w3m?action=checkblock&ip=%d.%d.%d.%d http://spamcop.net/w3m?action=checkblock&ip is the URL format for SpamCop's lookup page and *%d.%d.%d.%d* generates the IP address of the blocked host. The resulting protocol reply includes a URL that takes the blocked sender directly to SpamCop's lookup page and tests his or her IP address. **IMPORTANT:** If a percent sign (%) is provided as part of the SMTP message text, type it as %%. Using a single percent sign without the letter "d" might crash the SMTP Agent.
Delete	To remove an RBL site, select the site in the RBL list and click Delete.
Blocked Hosts	A list of blocked IP address ranges. If Do Not Allow Access from Hosts in Blocked List is selected, the SMTP Agent refuses connections from any host within the designated IP address range. Listing ranges of registered IP addresses blocks specific external hosts from sending mail to or relaying mail through your messaging system. For example, you can choose to list the IP addresses registered to public mail systems (such as Hotmail,* Yahoo,* and Juno*) because spammers frequently use these systems to relay UBE. Use this option to block internal hosts. By listing ranges of internal IP addresses, you can block specific workstations from sending any messages over the Internet.
Add	To add a range of IP addresses to the Blocked Hosts list, 1. Type a range of disallowed IP addresses. For example: 251.70.2.53-251.70.2.60 2. Click Add. Repeat for each additional range of disallowed IP addresses. If you are using WebAdmin, provide only one range per line.

Option	Function
Delete	To delete a range of IP addresses from the Blocked Hosts list, 1. Select the range. 2. Click Delete.
UBE Relaying	This page provides options that prevent spammers from using your messaging system to relay unsolicited bulk e-mail (UBE) or SPAM. Changes to these properties are implemented within 5 minutes.
Flags	
SMTP-after-POP	Prohibits users from sending remote messages through the SMTP Agent until they have first authenticated with the messaging system via their POP3 or IMAP4 client. This works for most Internet e-mail clients because these clients always check for e-mail (log in) just before sending messages. This feature also includes the username of the person who authenticated with the messaging system in the message header. This helps track spammers who authenticate with a valid username but fake the message header to mask their identity. SMTP-after-POP requires that you run the Connection Manager Agent and that you configure the Conn. Mgr. option on the messaging server running the SMTP Agent. See “SMTP-after-POP” on page 232 for detailed instructions on configuring SMTP-after-POP authentication.
Only Allow Remote Sending for Authenticated Senders	Enables Extended SMTP (ESMTP) authentication. If selected, the e-mail client must authenticate through the ESMTP protocol before the SMTP Agent relays its messages to remote recipients. Netscape Communicator* and Outlook* Express support ESMTP authentication. If both SMTP-after-POP and ESMTP authentication are enabled, they function as an either/or option. If a mail client does not authenticate via POP or IMAP when downloading mail, it must authenticate via ESMTP before it can send remote messages.
Require Sender to Be in Allowed List for Remote Sending	Restricts access to your NetMail system by selectively allowing access. If marked, only mail hosts with an IP address designated in the Allowed Hosts list can relay remote messages through the current SMTP server. If SMTP-after-POP, ESMTP authentication, and Require Sender to Be in Allowed List for Remote Sending are all enabled, they function as an either/or option. If an e-mail client does not authenticate using of POP or IMAP when downloading mail, it must authenticate using ESMTP or the Allowed Hosts list must include it before it can send remote messages.

Option	Function
Maximum Number of Recipients per mail	Restricts the number of users who can receive the same message. This option affects both inbound and outbound Internet messages. If a message exceeds the threshold, the SMTP Agent begins at the top of the recipient list and sends the message to the number of recipients designated in this field. You can also configure the ModWeb Mail Module to restrict the number of recipients per message sent by users in the Modular Web client. For information on the ModWeb Mail Module, see Table 4, "ModWeb Mail Module," on page 374.
Allowed Hosts	Includes a list of allowed IP address ranges. When the Require Sender to Be in Allowed List for Remote Sending option is selected, only hosts that fall within the designated IP address ranges are allowed to send messages to remote recipients via the current SMTP Agent. 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.
Allowed Hosts *continued*	In addition to preventing external hosts from relaying messages through your messaging system, you can use the Allowed Hosts list to prevent internal hosts from relaying remote messages. To restrict which workstations outside your organization that you allow to send remote messages, designate ranges of internal IP addresses. **NOTE:** If a workstation's IP address is not in an Allowed Hosts range, you can still use the workstation to send messages to users within the local messaging system.
Add	To add a range of IP addresses to the Allowed Hosts list, 1. Type a range of allowed IP addresses. For example: 251.70.2.53-251.70.2.60 2. Click 3. Add. Repeat for each additional range of allowed IP addresses. If you are using WebAdmin, provide only one range per line.
Delete	To delete a range of IP addresses from the list, 1. Select the range. 2. Click Delete.
Relayed Domains (ETRN)	ETRN Domains are messaging systems that use a hosting service, such as an ISP or ASP, to send and receive messages over the Internet. These systems have their own messaging servers, agents, and mail directories; however, all their messaging services are local. Consequently, they must use a hosting service to send and receive remote messages. In most instances, ETRN Domains have non-persistent dial-up connections to their ISP or ASP. For more information, see "Servicing ETRN Domains" on page 251.
Domain(s)	The current SMTP Agent services the ETRN Domains. To support these domains, you must click the Accept ETRN option in the Options page.

Option	Function
Queue Server	The queue server is the NMAP Agent to which the SMTP Agent delivers messages that the message queue needs to process. Each SMTP Agent can only have one queue server. Use the Browse button to select any NMAP Agent in the tree. If the SMTP and NMAP Agents are not running on the same server, you can designate the SMTP server as a trusted host of the NMAP Agent server for faster access. For more information, see the Trusted Hosts property in Table 4, “Configuring the NMAP Agent,” on page 68. To verify that a List Agent is registered to a particular queue server, view the Client property in the NMAP object. If registered, the server running the SMTP Agent is listed as an NMAP client. **IMPORTANT:** You must restart SMTPD to effect any changes in the Queue Server configuration. (See “Loading and Unloading NetMail Agents” on page 317 for more information.)
Monitored Queues	A monitored queue is the message queue from which the SMTP Agent picks up messages for remote delivery. Because NMAP Agents manage the message queues, monitored queues correspond to NMAP Agents. A single SMTP Agent can monitor multiple message queues. Use the Browse button to select one or more NMAP Agents. **NOTE:** You cannot configure multiple SMTP Agents to monitor the same queue. Only one SMTP Agent can monitor each queue. To verify that an SMTP Agent is registered to a particular message queue, view the Client property in the NMAP object. If registered, the server running the SMTP Agent is listed as an NMAP client. Changes to this property are implemented within 5 minutes.
NetMail Parent Object	The Parent object associated with the SMTP Agent. The SMTP Agent recognizes all Global and Hosting Domains listed in its associated Parent objects. See “Supporting Multiple Internet Domains” on page 247 for more information. Changes to this property are implemented within 5 minutes.
Status	By default, the SMTP Agent is enabled. To disable the SMTP Agent, 1. Mark Disable Agent. 2. Click OK. Marking Disable Agent prevents the messaging server from launching the SMTP Agent at startup. However, to immediately disable the agent, you must manually unload SMTPD.NLM or restart the messaging server. For more information on manually unloading NetMail agents or restarting the messaging server, see “Loading and Unloading NetMail Agents” on page 317. After the SMTP Agent is disabled, the messaging server does not launch SMTPD.NLM again until you deselect the Disable Agent option and restart the messaging server.

NDS Object Configuration Options

This section reviews the NetMail configuration options for the following NDS objects:

- Table 3, "Container Objects," on page 393
- Table 4, "Server Objects," on page 393
- Table 5, "User Objects," on page 394

For an overview of each object's function within NetMail, see "NetMail Attributes in Existing Directory Objects" on page 18.

Table 3 Container Objects

Option	Function
NetMail Options	
Message Store	The volume and, optionally, the directory where the mailboxes for users in the current container are located. If only a volume is designated, the mail directories are created at the root of the volume. Changes to this property are implemented within 5 minutes. **NOTE:** Only the users' mailbox directories are located in the container message store. The message queue and SCMS directories are always located in the default volumes and directories.
Domain	The domain assigned to the current container. Changes to this property are implemented immediately. Use Container Domains in conjunction with Global Domains; that is, if a Container Domain is defined, include it Container Domains are referenced by the Address Book Agent in returning users' address book information or in determining what address book contexts a user can access. (See "Address Book Agent" on page 106 for more information.) The Modular Web Agent can also use Container Domains to generate users' Internet e-mail addresses. (See "User E-mail Addresses" on page 195. **IMPORTANT:** Container Domains do NOT allow you to have non-unique user IDs in different containers.

Table 4 Server Objects

Option	Function
Syslog Configuration	**IMPORTANT:** You must restart the messaging server to effect changes in the Internet Services' Syslog configuration. For more information about restarting the messaging server, see "Loading and Unloading NetMail Agents" on page 317.

Option	Function
	The Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug options represent messaging server events. Mark the events you want syslog to track. **NOTE:** For more information on the Syslog utility and startup options, see "SYSLOG" on page 329
Log to file	Mark Log to file to write Syslog events to file. On NetWare systems, the default path and filename is sys:\ETC\SYSLOG.If a filename is specified in the log file field, the designated file is created in the sys:\ETC\SYSLOG.D directory on every messaging server in the tree. If a full path and filename are specified, the designated file and directory structure is created on every messaging server in the tree. On Windows systems, the default path and filename is <*windows directory*>\ system32\drivers\etc\syslog. If a filename is specified in the log file field, the designated file is created in the <*windows directory*>\ system32\drivers\etc\ directory on every messaging server in the tree. If a full path and filename are specified, the designated file and directory structure is created on every messaging server in the tree. On Linux, the Syslog is part of the operating system. It is typically configured by editing the /etc/syslog.conf file. The maximum syslog file size is 1MB. When the file exceeds 1 MB, it wraps.
Do not log	If selected, no log file is created.
Override global configuration with above settings	Overrides the default syslog configuration defined in the Internet Services container object with the server's syslog configuration. You must mark Override global configuration with above settings for the server's syslog configuration to take effect. Otherwise, the Internet Services' syslog configuration remains in effect.
NetMail Information	A view-only page indicating that a NetMail messaging server is running on the current server.

Table 5 User Objects

Option	Function
Identification	All changes to User object properties are implemented immediately.

Option	Function
Internet E-Mail Address	The user's Internet e-mail address. This address must include the user's complete e-mail address, including the domain. You can automatically populate this field using the Alias Agent's Internet E-mail Address feature. **NOTE:** ModWeb does not verify the domain listed in the User Object's Internet E-mail Address property is a supported Global or Hosting domain. Therefore, it is recommended you use the Alias Agent to populate this property or manually ensure the domain is valid. If the User object's Reply To Address field is empty, ModWeb uses the Internet E-Mail Address as the user's reply-to address. This address appears on the From: line of the user's outgoing mail. **IMPORTANT:** Typing the Internet E-Mail Address does NOT automatically enable the user to receive mail at this address. If the Internet E-Mail Address differs from the user's actual e-mail address, you must create an alias that associates the Internet E-Mail Address with the user's system e-mail address. You can either create an NDS Alias object or use the Alias Agent to create the alias. For more information, see "Managing User Aliases" on page 253. (You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create Alias objects.)
NetMail Configuration	All changes to User object properties are implemented immediately.
General	
Privacy	Sets the user's level of privacy within the messaging system. The privacy level controls what the Address Book Agent reveals about the user. The privacy options are executed as follows: ◆ **None**: The current user's e-mail address, first name, last name, and full name is returned in address book queries. ◆ **Limited**: Only the current user's e-mail address is returned in address book queries. ◆ **Unlisted**: The current user's personal information is not available.
Timeout	The amount of idle time before the user is automatically logged out of the Modular Web client. Specific actions, such as opening or sending an item, generate a call to the Web server. Other actions, such as scrolling through items in the Item List, composing a message without sending it, or reading Help topics, do not generate a call to the Web server. If, for a period of time, you leave the Modular Web client alone or perform actions that don't generate a call, the client logs you out. Doing so not only secures your mailbox, but it also ensures that the Web server and Modular Web client run efficiently. When you have timed out, and therefore are automatically logged out, and you attempt to perform a function, you are prompted to log in again. If you are logged out while composing a message, NetMail prompts you with a login dialog when you attempt to send the message or go to another page, If you login successfully, NetMail resumes the original session so the message is not lost. You can type a value (in minutes) between 1 and 40.

Option	Function
Reply To Address	The user's preferred reply-to address. The reply-to address appears on the From: line of the user's outgoing mail. **IMPORTANT:** Typing the Reply To Address does NOT automatically enable the user to receive mail at this address. If the reply-to address differs from the user's actual e-mail address, you must create an alias that associates the reply-to address with the user's system e-mail address. You can user either an NDS Alias object or the Alias Agent to create the alias. For more information, see "Managing User Aliases" on page 253. (You cannot create Alias objects in WebAdmin; therefore, you must use another administrative tool, such as iManager, to create Alias objects.) If this field is left empty, ModWeb uses the Internet E-mail Address attribute from the User object as the user's Reply To address. **NOTE:** ModWeb does not verify the domain listed in the User Object's Internet E-mail Address property is a supported Global or Hosting domain. Therefore, it is recommended you use the Alias Agent to populate this property or manually ensure the domain is valid. If the Internet E-mail Address property is not configured in the User object, ModWeb dynamically generates the user's e-mail address as follows: 1. If the user belongs to a Hosting Domain, ModWeb simply uses the username as the e-mail address. 2. If the user belongs to a Global Domain, ModWeb generates the e-mail address from the username and the user's Internet domain (username@domain). To identify the user's Internet domain, ModWeb looks in the following objects: a.If the user is associated with a Parent object, ModWeb looks in the Parent object's Global Domains list. b.If no Global Domain is configured in the Parent object, ModWeb looks for the user's Container Domain. c.If no Container Domain is configured, ModWeb uses the messaging server's Official Domain. Changes to this property are implemented immediately.
Forwarding	Enables the user to forward their incoming messages to another e-mail address. The AutoReply Agent must run a messaging server within the user's messaging system for this option to function.
Forward Mail to	The e-mail address where the user's incoming messages are forwarded. Mark the Forward Mail To option to forward the user's incoming messages to the designated e-mail address.
Keep Local Copy	Keeps a copy of all forwarded messages in the user's NetMail mailbox. If Keep Local Copy is not marked, incoming messages are simply forwarded; they are not delivered to the user's mailbox.

Option	Function
AutoReply/Vacation	Enables the user to create a custom message that is sent in response to incoming messages.
Reply to all received mail with message	The current user's autoreply/vacation message. Mark Reply to all received mail with message to send the autoreply/ vacation message in response to incoming messages.
Store	
User Disabled	Excludes the current user from the messaging system. Though the user might reside in a supported NMAP context, selecting this option prevents the user from sending or receiving mail through NetMail. **NOTE:** This option only affects the NetMail messaging system. It does not disable the User object in NDS.
Disk Quota (kByte)	The user's mailbox quota. The user's messages, folders, and calendar items count against the mailbox quota. This property overrides the System-Wide Mailbox Quota set in the NMAP Agent. For the Disk Quota to take effect, you must mark the Per User Mailbox Quotas option in the NMAP Agent's configuration or the user's Parent object must defer the mailbox quota setting to the User object. Use the Disk Quota property to allot additional mailbox space on a case-by-case basis (e.g. system administrators, the messaging server's postmaster, or company VIPs).
NetMail Proxy Configuration	Enables the user to retrieve messages from up to three POP3 or IMAP4 e-mail accounts on other messaging systems. All changes to User object properties are implemented immediately.
Entry	The currently displayed Proxy entry. A user can have up to three proxy entries.
Type	The target account's e-mail protocol. Select POP3 or IMAP4.
Leave Mail on Server	Leaves a copy of all proxied messages in the target account's mailbox. If Leave Mail on Server is not marked, proxied messages are deleted from the target account's mailbox.
Host	The host name or IP address of the target account's POP or IMAP server. You need to know the Host Name of the POP or IMAP server for your service provider, such as imap.myisp.com, mail.myisp.com, or pop.mail.myisp.com. If you do not know the host name, contact your service provider.For example, the host name format is imap.myisp.com, mail.myisp.com, or pop.mail.myisp.com. If you do not know the host name, contact your service provider.
User Name	The username for the target account.
Password	The password for the target account.
Clear	Clears the current proxy entry.

Option	Function
NetMail Parent Object	The Parent object associated with the current user. The user “inherits” all options configured in the Parent object unless Use user configuration, fallback to parent configuration is marked in the Parent object. This option gives User object settings precedence over the Parent object. Use Ctrl+Click o simultaneously configure this property for multiple users and access the Details page. For more information, see “Configuring Multiple User Objects Simultaneously” on page 208. All changes to User object properties are implemented immediately.
IMAP	All changes to User object properties are implemented immediately.
IMAP Access	Enables or disables IMAP connections for the current user. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
POP	All changes to User object properties are implemented immediately.
POP Access	Enables or disables POP connections for the current user. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
Forward	All changes to User object properties are implemented immediately.
Forward Ability	Enables or disables message forwarding for the current user. If Enabled is selected, the User object’s Forwarding settings are activated. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the agent is enabled. **NOTE:** If Forwarding properties are defined in both the User and Parent objects, precedence is determined by the Parent object’s Default Inheritance setting.
Forwarding	
Forward Mail To	The e-mail address where incoming messages are forwarded. Mark the Forward Mail To option to forward all messages received by the current user to the designated e-mail address.
Keep Local Copy	Keeps a copy of all forwarded messages in the user’s mailbox. If Keep Local Copy is not marked, incoming messages are forwarded and deleted from the user’s mailbox.
AutoReply	All changes to User object properties are implemented immediately.
AutoReply Ability	Enables or disables AutoReply messages for the current user. If Enabled is selected, the User object’s AutoReply/Vacation settings are activated. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the agent is enabled. **NOTE:** If AutoReply/Vacation properties are defined in both the User and Parent objects, precedence is determined by the Parent object’s Default Inheritance setting.
AutoReply/Vacation	

Option	Function
Reply to all received mail with message	Sends the defined autoreply message in response to all messages received by the current user. The autoreply message is only sent to the original sender; not all message recipients.
Messaging Rules	All changes to User object properties are implemented immediately.
Rule Usage Ability	Enables or disables the Rules feature for the current user. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
Task Oriented Management	Allows the administrator to give the current user rights to create, import, modify, or delete user accounts in the domains and contexts designated in the associated Parent object. For more information, see "Task-Oriented Management" on page 196. All changes to Task Oriented Management properties are implemented immediately. **NOTE:** All task-oriented management functions are enabled by the Modular Web Agent Task Management Module. Although the module itself has no configurable options, to provide TOM functionality via WebAccess, it must run on the messaging server.
General	
Parent Objects	The Parent object(s) with which the current TOM administrator is associated. In the WebAccess interface, the TOM administrator is able to create, modify, delete, or import users in the Global or Hosting Domains associated with the selected Parent object(s). User objects are created in the NMAP context(s) designated in the Parent object. For more information, see the Managed context properties in Table 4, "Parent Object," on page 352.
Rights	
Allow user creation	The TOM administrator can create User objects in the NMAP context(s) listed in the Parent object. If multiple contexts are listed in the Parent object, NetMail equally distributes new User objects between the contexts. In creating the user account, the TOM administrator can select one of the domains listed in their Parent object's Managed domain names property. Use this domain to create the new user's Internet e-mail address (username@domain). If the TOM administrator selects multiple domains when creating the user, the User object is created with the first domain name and Alias objects are created with the subsequent domain names. For example, if the TOM administrator selects domains abc.com and 123.com when creating a user account for jotero, the User object is created as jotero@abc.com. The Alias object, jotero@123.com, points to jotero@abc.com. **IMPORTANT:** When creating usernames, do not use extended characters in Internet e-mail addresses or users cannot access the messaging system or receive messages. Make sure to inform TOM administrators not to use extended characters in usernames.

Option	Function
Allow user import	The TOM administrator can import users using comma-delimited, ASCII files. The new User objects are created in the NMAP context listed in the Parent object. If multiple contexts are listed in the Parent object, NetMail equally distributes new User objects between the contexts.
Allow user import *continued*	The first line in the import file is a header row of sorts. It specifies the attributes you are importing and the order you want them to appear in the user records. Of these attributes, the first three are fixed. ◆ For users belonging to Global Domains, attribute 1 is the username. For users belonging to Hosting Domains, attribute 1 is the full e-mail address (username@hosted_domain.com). The TOM module verifies each Hosting Domain before allowing the import. If the TOM administrator doesn't have rights to a given user's domain (i.e. the Hosting Domain isn't listed in the Parent object's Managed domain names property), TOM errors out the import and proceeds to the next user in the list. ◆ Attribute 2 is the surname. ◆ Attribute 3 is the password. Aside from these fixed attributes, the import file can include any data—not just WebAccess-specific attributes. For example, the first line or header row of the import file can appear as follows: Username, Surname, Password, First name, Middle Initial Following the header row are the user records. Each line represents a different user record. The data in each record is delineated by commas and must appear in the order designated in the header row. Using the header row from the previous example, a user record would appear as follows: simon@test.com, Roberts, ih8beets, Simon, T
Allow user deletion	The TOM administrator can delete users from the NMAP context(s) selected in the Parent object. When a TOM administrator deletes a user account, they are given the option of removing the user's mailbox and all associated directories.
Enable domain settings	The TOM administrator can define default user attributes. These attributes are applied to all users created or imported in *any* of the domains designated in the Parent object.
Calendar/Scheduling	Changes to this property are implemented immediately.
Calendar Access	Enables or disables the user's Calendar(s) and scheduling functions. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the calendar and scheduling options are enabled.
Modular Web Agent	Changes to this property are implemented immediately.
Modular Web Access	Enables or disables the ModWeb client for the current user. If Enabled is selected, the User object's Default Timezone setting is activated. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the agent is enabled.

Option	Function
Default Timezone	The default time zone for the Modular Web Agent and its sub-modules. **NOTE:** If the Default Timezone is defined in both the User and Parent objects, precedence is determined by the Parent object's Default Inheritance setting. If the Default Timezone is defined in User Preferences, the User Preference setting takes precedence over both the Parent and User object settings.
Calendar Agent	All changes to User object properties are implemented immediately.
CalAgent Ability	Enables or disables iCal functionality, including automatic event status tracking, for the current user. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the agent is enabled.
AntiVirus	Changes to this property are implemented immediately.
Virus scanning	Allows the administrator to enable or disable virus scanning for the current user. Selecting Deferred defers the setting to the Parent object. If Deferred is selected in both the Parent and User objects, the agent is enabled.

Quick Reference Matrix

The following matrix provides a quick reference of commands, file structure, and available utilities for each supported operating system.

Table 3 NetMail Quick Reference Matrix

	NetWare	Windows	Linux
Binary Directory	sys:\system	\program files\novell\ netmail\bin	/opt/novell/netmail/bin/
Commands	MAIL	MAILCON	NMAIL
IMSAudit Output Directory	sys:\novonyx\mail\dbf b	c:\program files\novell\netmail\dbf b	/var/opt/novell/netmail/dbf
Log File	sys:\etc\syslog	\<*windows directory*>\ system32\drivers\etc\syslog	/var/opt/novell/naudit/logs
Mail Store	sys:\novonyx\mail	\program files\novell\ netmail\mail	/var/opt/novell/netmail/
Mailbox Directories	sys:\novonyx\mail\users\	\program files\novell\ netmail\mail\users	/var/opt/novell/netmail/users/
SCMS Directories	sys:\novonyx\mail\scms\	\program files\novell\ netmail\ mail\scms\	/var/opt/novell/netmail/scms/
Message Queue	sys:\novonyx\mail\spool\	\program files\novell\ netmail\ mail\spool	/var/opt/novell/netmail/spool/

a Depending on configuration.

b These default directories are defined in the Messaging Server object.

	NetWare	Windows	Linux
Server Utilities	MAILCON	DBF directoryb	DBF directoryb
	SYSLOG	SYSLOG	
	IMSAUDIT	IMSAUDIT	IMSAUDIT
	NIMSEXT	NIMSEXT	nimsext.sh
	AUDITEXT	AUDITEXT	auditext.sh
	MAIL LOAD		
	RMBOX	RMBOX	RMBOX
NetMail OpenSSL Certificates	sys:\system\osslcert.pem	*drive*:\program files\novell\netmail\dbf\osslcert.pem	/var/opt/novell/netmail/dbf/osslcert.pem
NetMail OpenSSL Key Files	sys:\system\osslpriv.pem	*drive*:\program files\novell\netmail\dbf\osslpriv.pem	/var/opt/novell/netmail/dbf/osslpriv.pem
WebAdmin OpenSSL Certificates	sys:\system\webadmin\osslcert.pem	*drive*:\program files\novell\webadmin\osscert.pem	/opt/novell/WebAdmin/osslcert.pem
WebAdmin OpenSSL Key Files	sys:\system\webadmin\osslpriv.pem	*drive*:\program files\novell\webadmin\osspriv.pem	/opt/novell/WebAdmin/osslpriv.pem
Startup Commands	load ims	Start the NetMail Manager Service	/etc/init.d/novell-netmail start
Stop Commands	ims u	Stop the NetMail Manager Service	/etc/init.d/novell-netmail stop
Template Directory	sys:\system\modweb	\program files\novell\netmail\bin\modweb	/opt/novell/netmail/bin/modweb/

a Depending on configuration.

b These default directories are defined in the Messaging Server object.