Novell GroupWise®

6.5

www.novell.com

ADMINISTRATION GUIDE

February 6, 2006

Novell®

Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

GroupWise 6.5 Administration Guide
February 6, 2006

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

Novell Trademarks

Third-Party Materials

Contents

Part IV Users

Part XI Internet Agent

Part XIII Monitor

Part XV Security

About This Guide

This Novell® *GroupWise® 6.5 Administration Guide* helps you maintain all components of your GroupWise system. The guide is divided into the following sections:

Additional Documentation

For additional GroupWise documentation, see the following guides at the Novell GroupWise 6.5 documentation Web site (http://www.novell.com/documentation/gw65):

- *Installation Guide*
- *Multi-System Administration Guide*
- *Interoperability Guide*
- *Troubleshooting Guide*s
- *GroupWise Client User Guides*

Documentation Updates

For the most recent version of the *GroupWise 6.5 Administration Guide*, visit the Novell GroupWise 6.5 documentation Web site (http://www.novell.com/documentation/gw65).

Documentation Conventions

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

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

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

I

System

1 GroupWise System Administration

As a GroupWise® system administrator, it is your responsibility to keep your GroupWise system running smoothly for your GroupWise users. This *GroupWise 6.5 Administration Guide* provides a wealth of information to help you accomplish this task. This System section provides an overview of the GroupWise administration tool, ConsoleOne®, and its capabilities. It summarizes administrative tasks that affect your GroupWise system as a whole and provides links to more specialized instructions.

The following sections of the *Administration Guide* detail the eDirectory™ objects where GroupWise information is stored. Instructions are provided for creating and managing all GroupWise object types.

- "Domains" on page 107
- "Post Offices" on page 145
- "Users" on page 187
- "Resources" on page 221
- "Distribution Lists, Groups, and Organizational Roles" on page 235
- "Libraries and Documents" on page 261

The following sections of the *Administration Guide* detail the GroupWise software components that make your GroupWise system run. Instructions are provided for configuring, monitoring, and optimizing each software component.

- "Post Office Agent" on page 415
- "Message Transfer Agent" on page 555
- "Internet Agent" on page 659
- "WebAccess" on page 803
- "Monitor" on page 901

The following additional sections of the *Administration Guide* provide supporting details and background information:

- "Databases" on page 339
- "Security" on page 1031
- "Client" on page 963

2 ConsoleOne Administration Tool

GroupWise® is administered using ConsoleOne®, a Java*-based tool for managing your network and its resources. When you create your GroupWise system, GroupWise snap-ins are added to your ConsoleOne installation and GroupWise objects are created in Novell® eDirectory™. As you manage your GroupWise system, you use ConsoleOne to create additional GroupWise objects, modify GroupWise object properties, and so on.

IMPORTANT: Because the GroupWise snap-ins to ConsoleOne are required in order to work with GroupWise objects, you cannot use other network management tools, such as Novell iManager, to administer your GroupWise system. Also, you should not use older network management tools, such as NetWare Administrator, to administer your GroupWise system, unless your GroupWise system includes legacy gateways that require such tools to administer the corresponding Gateway objects and their properties.

Because GroupWise is a cross-platform product, you might have components of your GroupWise system located on NetWare® servers, Linux servers, and Windows* servers. You can run ConsoleOne on Windows or Linux to manage GroupWise domains and post offices located on any of these platforms.

- "ConsoleOne on Windows" on page 35
- "ConsoleOne on Linux" on page 36

NOTE: For a GroupWise system on NetWare, you cannot run ConsoleOne to administer GroupWise at the NetWare server console. The GroupWise Administrator snap-ins to ConsoleOne do not run in that environment.

ConsoleOne on Windows

You can run ConsoleOne on Windows on any Windows machine that meets the requirements listed in "GroupWise Administration Requirements" in the *GroupWise 6.5 Installation Guide*.

- "Installing ConsoleOne on Windows" on page 35
- "Starting ConsoleOne on Windows" on page 36

Installing ConsoleOne on Windows

When you create your initial GroupWise system using the GroupWise Installation program (install.exe) on Windows, the GroupWise snap-ins to ConsoleOne are installed to the ConsoleOne installation on that machine. If necessary, you can install ConsoleOne itself to the machine where you are running the GroupWise Installation program. You are also given the opportunity to copy the GroupWise snap-ins to ConsoleOne into a GroupWise software distribution directory for later use.

After you have set up your GroupWise system, you can use the GroupWise Installation program to install ConsoleOne and the GroupWise snap-ins from the *GroupWise 6.5 Administrator* CD or you can run admin\install.exe to install the snap-ins from the software distribution directory to additional locations as needed.

Starting ConsoleOne on Windows

When you install ConsoleOne, a ConsoleOne icon is automatically created on your Windows desktop for starting ConsoleOne.

ConsoleOne on Linux

You can run ConsoleOne on Linux on any Linux machine that meets the requirements listed in "GroupWise Administration Requirements" in the *GroupWise 6.5 Installation Guide*.

- "Installing ConsoleOne on Linux" on page 36
- "Starting ConsoleOne on Linux" on page 36

Installing ConsoleOne on Linux

When you create your initial GroupWise system using the GroupWise Installation program (install) on Linux, ConsoleOne should already be installed before you begin. Linux ConsoleOne is available on the Novell Downloads page (http://download.novell.com/index.jsp).

After ConsoleOne is installed, the GroupWise Installation program on Linux installs the GroupWise snap-ins to ConsoleOne to the ConsoleOne installation on that machine. You are also given the opportunity to copy the GroupWise Administration RPM into a GroupWise software distribution directory for later use.

After you have set up your GroupWise system, you can use the GroupWise Installation program to the GroupWise snap-ins from the *GroupWise 6.5 Administrator* CD or you can install the GroupWise Administration RPM from the admin subdirectory of the software distribution directory to install the snap-ins to additional locations as needed.

Starting ConsoleOne on Linux

1. In a terminal window, become root by entering **su** and the root password.
2. Enter the following command:

   ```
   /usr/ConsoleOne/bin/ConsoleOne
   ```

3 GroupWise View

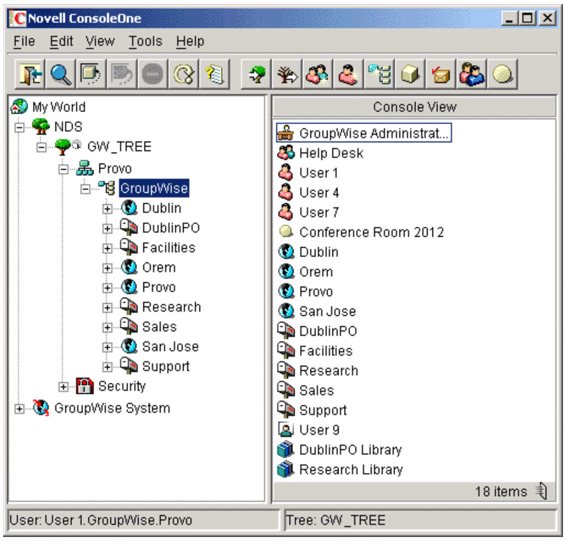
When administering GroupWise® in ConsoleOne®, you can use the standard Novell® eDirectory™ View or you can use the GroupWise View. The following sections discuss the GroupWise View and how to use it:

- "eDirectory View vs. GroupWise View" on page 37
- "GroupWise Object Icons" on page 38
- "Customizing the GroupWise View" on page 40
- "Searching in the GroupWise View" on page 42
- "Performing Administrative Tasks from the GroupWise View" on page 42

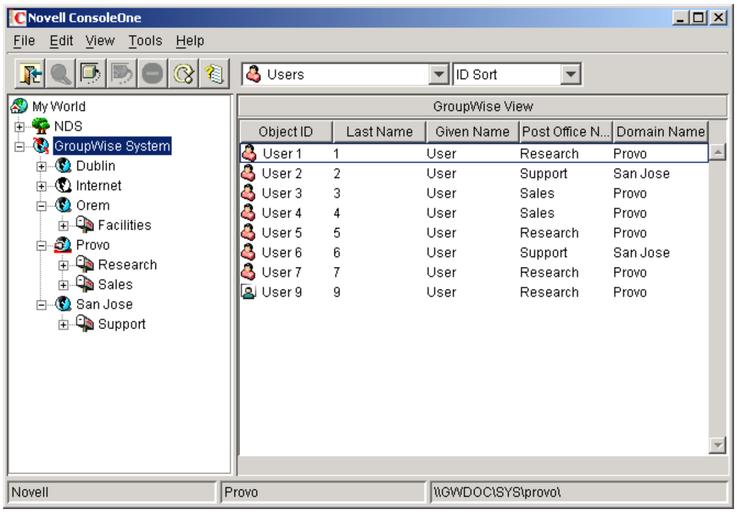
NOTE: The ConsoleOne images used in the guide show ConsoleOne on Windows. ConsoleOne on Linux displays slightly differently but provides substantially the same functionality.

eDirectory View vs. GroupWise View

The eDirectory View displays the GroupWise objects in their contexts in the eDirectory tree, as shown in the following example.



The GroupWise View filters out all non-GroupWise objects and shows how the GroupWise objects relate to each other in the GroupWise system, as shown in the following example.



Object ID	Last Name	Given Name	Post Office N...	Domain Name
User 1	1	User	Research	Provo
User 2	2	User	Support	San Jose
User 3	3	User	Sales	Provo
User 4	4	User	Sales	Provo
User 5	5	User	Research	Provo
User 6	6	User	Support	San Jose
User 7	7	User	Research	Provo
User 9	9	User	Research	Provo

In the left pane, all Domain objects are displayed under the GroupWise system, and all Post Office objects are subordinate to the domains where they reside. You can select the GroupWise system, a domain, or a post office in the left pane and then use the GroupWise Object list (located on the tool bar) to display associated objects (Users, Resources, Message Transfer Agents, and so forth) in the right pane. In the above example, the GroupWise System is selected in the left pane, the GroupWise Object list is set to Users, so the right pane is displaying all users in the entire GroupWise system.

GroupWise Object Icons

The following table lists all the GroupWise objects that are displayed in the eDirectory View or GroupWise View in ConsoleOne.

Icon	GroupWise Object	Additional Information
	GroupWise System	Represents the GroupWise system you are currently connected to. The GroupWise system's name is displayed in the lower left corner of the ConsoleOne window.
	Primary Domain	Represents the system's primary domain. To ensure consistency, all replication of GroupWise information to the GroupWise domain and post office databases takes place through the primary domain. For additional information, see "Domains" on page 107.
	Secondary Domain	Represents any additional domains, other than the primary, created in the GroupWise system. For additional information, see "Domains" on page 107.
	Current Domain	Represents the domain to which ConsoleOne is currently connected. For information about changing the current domain, see "Connecting to a Domain" on page 123.
	External Domain	Represents a domain from another GroupWise system.
	Non-GroupWise Domain	Represents all or part of a non-GroupWise system.

Icon	GroupWise Object	Additional Information
	Post Office	Represents a collection of user accounts (mailboxes). For additional information, see "Post Offices" on page 145.
	External Post Office	Represents a post office in an external GroupWise system or a non-GroupWise system.
	User	Represents an eDirectory user who has been given a GroupWise account on a post office. For additional information, see "Users" on page 187.
	External Entity	Represents a non-eDirectory user who has been given a GroupWise account on a post office. For additional information, see "Users" on page 187.
	External User	Represents a user in an external GroupWise system or a non-GroupWise system.
	Resource	Represents a conference room or some other resource that can be scheduled by users. For additional information, see "Resources" on page 221.
	External Resource	Represents a resource that belongs to an external GroupWise system or a non-GroupWise system.
	Distribution List	Represents a group of users or resources that can all be addressed by using the distribution list's name. For additional information, see "Distribution Lists, Groups, and Organizational Roles" on page 235.
	Group	Represents an eDirectory group. eDirectory groups, like distribution lists, can be addressed by using the group's name. Any members of the group who have GroupWise accounts receive the message. For additional information, see "Distribution Lists, Groups, and Organizational Roles" on page 235.
	Organizational Role	Represents an eDirectory organizational role. eDirectory organizational roles, like distribution lists, can be addressed by using the organizational role's name. Any members of the role who have GroupWise accounts receive the message. For additional information, see "Distribution Lists, Groups, and Organizational Roles" on page 235.
	Library	Represents a collection of documents. For additional information, see Chapter 21, "Document Management Services Overview," on page 263.
	Nickname	Represents an additional address associated with a user, resource, or distribution list. For additional information, see "Users" on page 187, "Resources" on page 221, or "Distribution Lists, Groups, and Organizational Roles" on page 235.
	Message Transfer Agent	Represents a Message Transfer Agent (MTA) associated with a domain. For additional information, see "Message Transfer Agent" on page 555.

Icon	GroupWise Object	Additional Information
	Post Office Agent	Represents a Post Office Agent (POA) associated with a post office. For additional information, see "Post Office Agent" on page 415.
	Gateway	Represents a method of linking to another e-mail system or transport. For additional information, see the GroupWise gateway guides.

Customizing the GroupWise View

You can change the column display, order, and width to customize the GroupWise View.

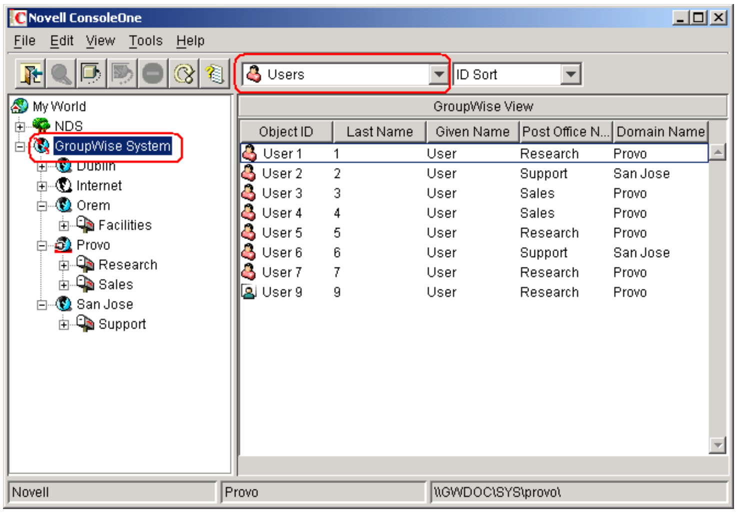
Changes are preserved from one ConsoleOne session to the next. In addition, your last view is persistent from session to session. For example, if you last used the Distribution Lists view, the next time you start ConsoleOne and open the GroupWise View, the Distribution Lists view is displayed. If the last-used view is not applicable (for example, you had the Gateways view open and when the new ConsoleOne session starts you select a Post Office object), the GroupWise View defaults to the Users view.

- "Changing the Column Display and Order" on page 40
- "Changing the Column Widths" on page 41

Changing the Column Display and Order

For each view (Users, Distribution Lists, Gateways, Post Offices, and so forth), you can determine which columns are displayed and the order in which they are displayed.

1 Select GroupWise System in the left (tree) pane, then select the view (for example, Users).



Users ID Sort

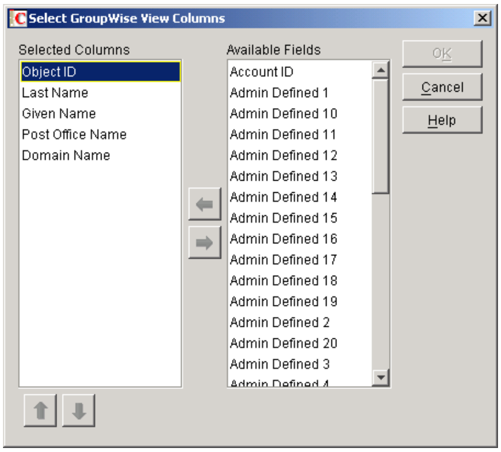
GroupWise View

Object ID	Last Name	Given Name	Post Office N...	Domain Name
User 1	1	User	Research	Provo
User 2	2	User	Support	San Jose
User 3	3	User	Sales	Provo
User 4	4	User	Sales	Provo
User 5	5	User	Research	Provo
User 6	6	User	Support	San Jose
User 7	7	User	Research	Provo
User 9	9	User	Research	Provo

2 If you are changing the Users view, select which view (ID Sort, User Name Sort, First Name Sort, or Last Name Sort) you want to change.

The Users view allows you to sort by ID, user name, first name, or last name. Each of these is treated as a separate Users view for which you can determine the column display and order.

3 Click the View menu > Edit Columns to display the Select GroupWise View Columns dialog box.



4 To add a column, select the column in the Available Fields list, then click the left arrow to add it to the Selected Columns list.

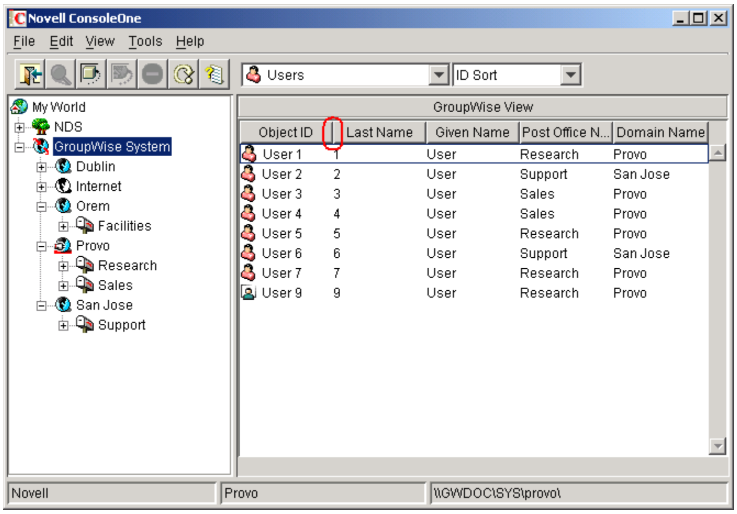
5 To determine the display order, select a column in the Selected Columns list, then click the up arrow and down arrow to move it to the desired position.

6 To remove a column, select the column in the Selected Columns list, then click the right arrow to add it to the Available Fields list.

7 When you are finished, click OK to save your changes.

Changing the Column Widths

You can change column widths in a view by dragging the right or left edge of the column label.



Object ID	Last Name	Given Name	Post Office N...	Domain Name
User 1	1	User	Research	Provo
User 2	2	User	Support	San Jose
User 3	3	User	Sales	Provo
User 4	4	User	Sales	Provo
User 5	5	User	Research	Provo
User 6	6	User	Support	San Jose
User 7	7	User	Research	Provo
User 9	9	User	Research	Provo

Searching in the GroupWise View

You can search for a specific entry in a view. The search is performed on the first column. For example, if the Resources view is displayed, you can search for a specific resource based on its object ID. If the Users view (with Last Name Sort selected) is displayed, you can search for a specific user based on the user's last name.

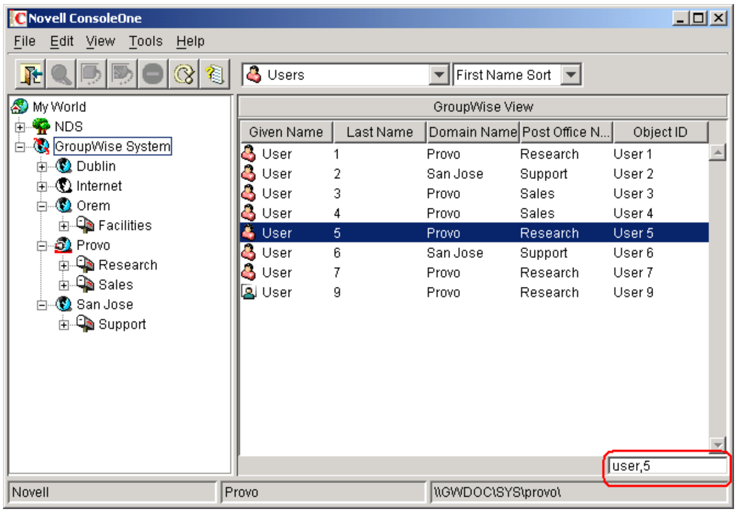
With the Users view, if you have First Name Sort or Last Name Sort selected, you can search for a complete user name (both first and last name) by using a comma as a delimiter between the names. A space after the comma is optional.

For example, if the User view displays first names in the first column and last names in the second column, you can type John,Smith to go directly to that user name. If the columns were reversed, you could use Smith,John.

To perform a search:

1. Change to the view you want to search.
2. Select the first entry in the view.
3. Type the text to search for.

   As you type text, a text box appears in the lower-right corner of the GroupWise View.



Given Name	Last Name	Domain Name	Post Office N...	Object ID
User	1	Provo	Research	User 1
User	2	San Jose	Support	User 2
User	3	Provo	Sales	User 3
User	4	Provo	Sales	User 4
User	5	Provo	Research	User 5
User	6	San Jose	Support	User 6
User	7	Provo	Research	User 7
User	9	Provo	Research	User 9

user,5

Novell | Provo | \\GWDOC\SYS\provo\

Performing Administrative Tasks from the GroupWise View

You can perform many GroupWise administrative tasks from the GroupWise View as well as from the eDirectory View. For example, you can:

- Create new objects.
- Modify the properties of an object.
- Move, rename, or delete an object from the GroupWise system.
- Use the GroupWise utilities, system operations, and diagnostic options on the Tools menu.

In addition, external objects must be created and managed in the GroupWise View because they are, by definition, external to eDirectory and have no eDirectory context. For example, if you install the GroupWise Internet Agent and want to simplify addressing for your users by adding the Internet as a non-GroupWise domain, you would need to perform the task in the GroupWise View.

4 System Operations

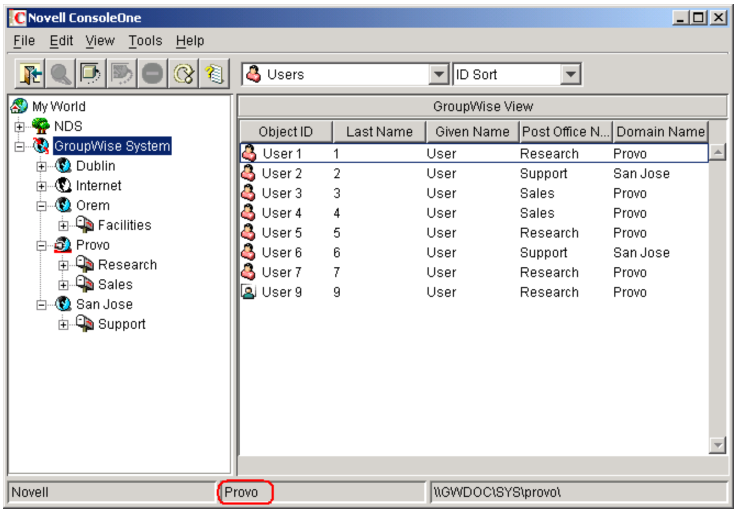
The GroupWise® system operations in ConsoleOne® allow you to perform various tasks to maintain and optimize your GroupWise system. The following sections provide information about the system operations included on the Tools menu (Tools menu > GroupWise System Operations):

NOTE: If the majority of the items on the GroupWise System Operations menu are dimmed, you are connected to a secondary domain in a GroupWise system where Restrict System Operations to Primary Domain has been selected under System Preferences. For more information, see "System Preferences" on page 44.

Select Domain

By default, ConsoleOne must be connected to a GroupWise domain in order for you to administer your GroupWise system. Being connected to a GroupWise domain ensures that information is replicated not only in Novell® eDirectory™ but also in the GroupWise domain and post office databases.

You can be connected to any domain in the GroupWise system. As shown in the following example, the domain to which you are connected is indicated by a plug on the domain's icon. In addition, the connected domain is listed at the bottom of the ConsoleOne window.



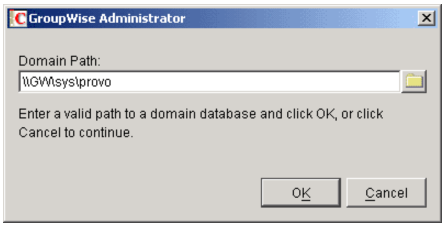
Object ID	Last Name	Given Name	Post Office N...	Domain Name
User 1	1	User	Research	Provo
User 2	2	User	Support	San Jose
User 3	3	User	Sales	Provo
User 4	4	User	Sales	Provo
User 5	5	User	Research	Provo
User 6	6	User	Support	San Jose
User 7	7	User	Research	Provo
User 9	9	User	Research	Provo

Some administrative tasks require you to be connected to a specific domain while others do not. In general, operations that create new GroupWise objects or delete GroupWise objects require you to be connected to the domain where the object resides. ConsoleOne uses the domain's UNC path (Domain object > GroupWise tab > Identification page) to automatically connect you to the correct domain if possible; otherwise, you must manually connect to the domain. Operations that simply modify the properties of an existing object do not require you to be connected to the object's domain.

NOTE: When you connect to a domain on a Linux server, a UNC path is still used but, because it is a Linux server, the first item in the UNC path is interpreted as the Linux server's hostname, followed by the path to the domain directory.

To change the domain to which you are connected:

1 In ConsoleOne, click the Tools menu > GroupWise System Operations > Select Domain.



Domain Path: \\GW\sys\provo

Enter a valid path to a domain database and click OK, or click Cancel to continue.

2 Browse to and select the domain directory, then click OK to connect to the domain.

NOTE: You can also connect to a domain by right-clicking the domain in the GroupWise View and selecting Connect.

System Preferences

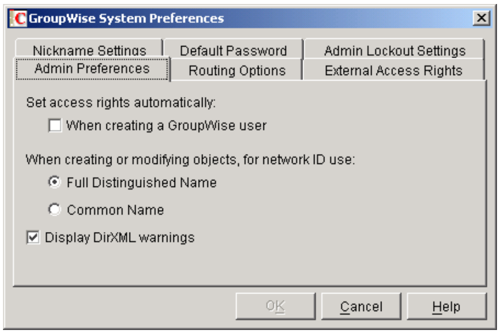
You can use the GroupWise system preferences to configure the defaults for several GroupWise system settings, including:

- Whether to assign the required eDirectory and file system rights to users when you create their GroupWise accounts. By default, rights are assigned automatically.
- Whether to use the fully distinguished name or common name for a user's network ID. By default, the fully distinguished name is used.

- The domain to assign as the default domain for any messages whose address cannot be resolved. By default, no domain is assigned.
- Whether your GroupWise system allows Busy Search and status tracking information to be returned to users on external GroupWise systems. By default, information is not returned.
- Whether to create a nickname (representing the object's old address) when moving an object from one post office to another. By default, nicknames are not automatically created.
- On Linux, the mount directory where ConsoleOne can find mount points for mounted file systems where domains and post offices are located.

To change the system preferences:

1. In ConsoleOne, click the Tools menu > GroupWise System Operations > System Preferences.



Set access rights automatically:

□ When creating a GroupWise user

When creating or modifying objects, for network ID use:

● Full Distinguished Name

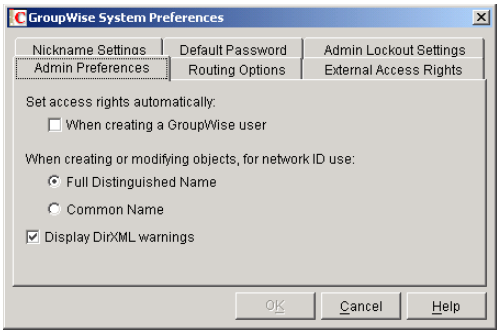
○ Common Name

☑ Display DirXML warnings

The GroupWise System Preferences dialog box contains the following tabs:

- **Admin Preferences:** Controls how rights are assigned and what network ID format is used when creating new GroupWise users.
- **Routing Options:** Controls default message routing for your GroupWise system.
- **External Access Rights:** Controls the access that users on external GroupWise systems have to your GroupWise users' information.
- **Nickname Settings:** Controls what happens when you move a user from one post office to another.
- **Default Password:** Assigns a default password for new GroupWise user accounts.
- **Admin Lockout Settings:** Controls access to the GroupWise administration functions in ConsoleOne.
- **Linux Settings (Linux Only):** Establishes the mount directory where ConsoleOne can find mounted file systems where domains and post offices are located.

2. Click the Admin Preferences tab to modify any of the following options:



Set access rights automatically:

□ When creating a GroupWise user

When creating or modifying objects, for network ID use:

● Full Distinguished Name

○ Common Name

☑ Display DirXML warnings

Set Access Rights Automatically: Users require specific eDirectory and file system rights in order to use GroupWise (see Chapter 86, “GroupWise User Rights,” on page 1067). Select this option to automatically grant these rights when creating a GroupWise account for users.

Appropriate eDirectory object rights enable the GroupWise client to log in to the user’s post office without prompting the user for the post office location (IP address, UNC path, or mapped drive.)

Appropriate file system rights enable the GroupWise client to directly access the post office directory rather than use client/server access.

When Creating or Modifying Objects, For Network ID Use: Select Full Distinguished Name (for example, paul.engineering.ny) when users’ mailboxes reside on a NetWare® 4.1*x* server (or higher) and users have an eDirectory connection to the server where the post office resides.

Select Common Name (for example, paul) under the following circumstances:

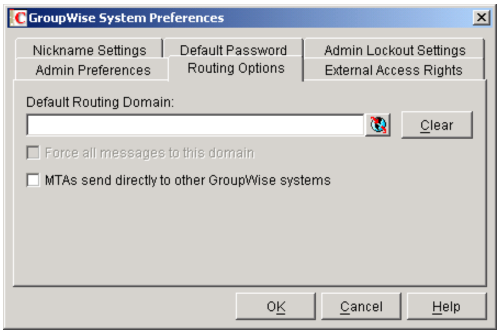
- The users’ mailboxes reside on a NetWare 3.1 server.
- The users’ mailboxes reside on a NetWare 4.1*x* server but users have a bindery emulation connection to the server where the post office resides.
- Users’ GroupWise IDs are different from their NetWare IDs.

Display DirXML Warnings: The DirXML® Driver for GroupWise provides data integration between GroupWise users and groups in eDirectory. For example, you can have an e-mail account automatically created as soon as an employee is hired. The same driver can also disable an e-mail account when a user is no longer active.

If you are using the DirXML Driver for GroupWise, some GroupWise operations that you perform in ConsoleOne® require you to take preliminary actions with the driver. For example, if you recover a deleted account, you need to stop the driver before recovering the account and restart it after the operation is complete.

This option enables you to receive a warning message whenever you perform a GroupWise operation in ConsoleOne that is affected by the DirXML driver. The warning message includes instructions about the actions you need to take with the driver before continuing with the GroupWise operation. If you are using the DirXML Driver for GroupWise, we strongly recommend that you enable this option. If you are not using the driver, you can disable the option to avoid receiving unnecessary messages.

3 Click the Routing Options tab to modify any of the following options:



Default Routing Domain:

□ Force all messages to this domain

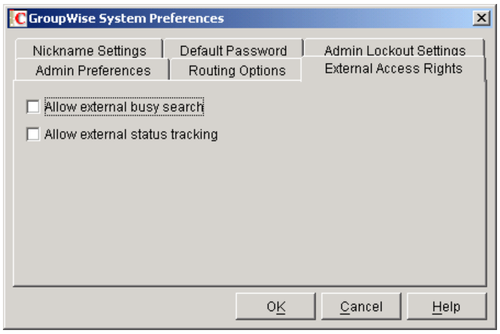
□ MTAs send directly to other GroupWise systems

Default Routing Domain: If a domain's MTA cannot resolve a message's address, the message is routed to this default domain's MTA. The default domain's MTA can then be configured to handle the undeliverable messages. This might involve routing the message to another GroupWise domain or to an Internet address (by performing a DNS lookup). Browse to and select the GroupWise domain you want to use as the default routing domain.

Force All Messages to this Domain: This option applies only if you select a default routing domain. Select this option to force all messages to be routed through the default routing domain regardless of the links you have configured for your GroupWise system's domains.

MTAs Send Directly to Other GroupWise Systems: Select this option if you want all MTAs in your GroupWise system to perform DNS lookups and route messages out across the Internet. If you deselect this option, you can designate individual MTAs to perform DNS lookups and route messages to the Internet.

4 Click the External Access Rights tab to modify any of the following options:



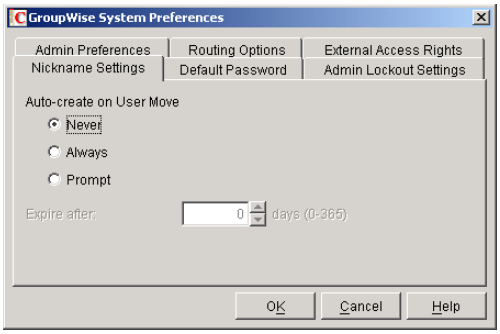
□ Allow external busy search

□ Allow external status tracking

Allow External Busy Search: Select this option to enable users in other GroupWise systems to perform Busy Searches on your GroupWise users' Calendars.

Allow External Status Tracking: Select this option to enable users in other GroupWise systems to receive message status information (such as whether a message has been delivered, opened, and so on) when messages arrive in your GroupWise system.

5 Click the Nickname Settings tab to modify any of the following options:



Auto-create on User Move

● Never

○ Always

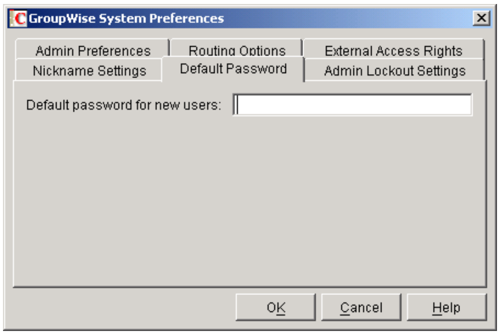
○ Prompt

Expire after: 0 days (0-365)

Auto-Create on User Move: A nickname is an alternative address that can be associated with a user. Whenever you move a user, GroupWise can automatically create a nickname with the user's old name and old post office. This enables messages sent to the old name to be automatically forwarded to the user's new address. Select whether or not you want GroupWise to never create nicknames, always create nicknames, or prompt you during the move process.:

Expire After: This option applies only if you selected Always or Prompt. If you want the nickname to be automatically removed after a period of time, specify the time period (in days). Valid values range from 1 to 365 days. A setting of 0 indicates that the nickname will not be automatically removed after the specified time period.

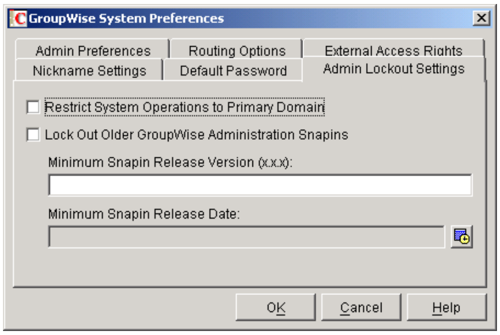
6 Click the Default Password tab to modify any of the following options:



Default password for new users:

Default Password for New Users: Specify the default password you want assigned to new GroupWise user accounts.

7 Click the Admin Lockout Settings tab to modify any of the following options:



□ Restrict System Operations to Primary Domain

□ Lock Out Older GroupWise Administration Snapins

Minimum Snapin Release Version (x.x.x):

Minimum Snapin Release Date:

Restrict System Operations to Primary Domain: Enable this option to allow an administrator to perform system operations (Tools menu > GroupWise System Operations) only when he or she is connected to the primary domain. All operations, except Select

Domain, Pending Operations, and Restore Area Management are unavailable when connected to a secondary domain.

Lock Out Older GroupWise Administration Snap-Ins: Enable this option to prevent administrators from using older GroupWise ConsoleOne snap-ins for accessing GroupWise objects in eDirectory. You can override these system lockout settings for individual domains (Domain object > GroupWise tab > Admin Lockout Settings page).

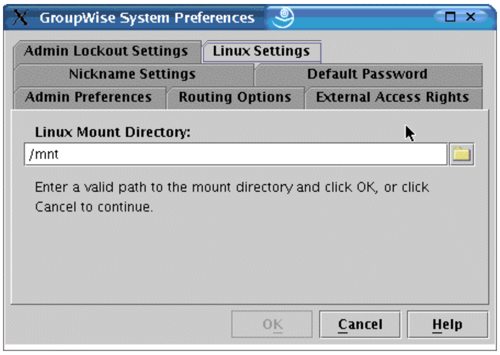
There are four GroupWise snap-ins to ConsoleOne, one for general administration, one for Internet Agent administration, and two for WebAccess administration. The ability to lock out older GroupWise snap-ins starts with GroupWise 6.5.

In the Minimum Snap-In Release Version (x.x.x) field, specify the version number of the oldest GroupWise snap-ins that can be used to administer your GroupWise system.

In the Minimum Snap-in Release Date, select the date of the oldest GroupWise snap-ins that can be used to administer your GroupWise system.

You can specify the minimum version, the minimum date, or both. If you specify both minimums, any administrator using snap-ins that are older than both minimums cannot use the GroupWise snap-ins. However, such an administrator can still run ConsoleOne for other purposes but must update the GroupWise snap-ins before GroupWise administration features are available again.

8 On Linux, click the Linux Settings tab to specify the mount directory.



Linux Mount Directory: /mnt

Enter a valid path to the mount directory and click OK, or click Cancel to continue.

Mount Directory: Specify the mount directory where ConsoleOne can find mounted file systems where domains and post offices are located.

GroupWise databases can be located on Linux servers, NetWare servers, or Windows servers. In the Linux mount directory, you create directories that have the same names as the servers that are mounted to those mount points. You do this for each server where a domain or post office is located that you want to access from ConsoleOne.

GroupWise administrators can have different mounts points depending on the workstation or server where they are running ConsoleOne. The mount directory information is stored in a user-specific preferences file (.consoleone/SnapinPrefs.ser in each GroupWise administrator's home directory).

9 Click OK to save the changes.

eDirectory User Synchronization

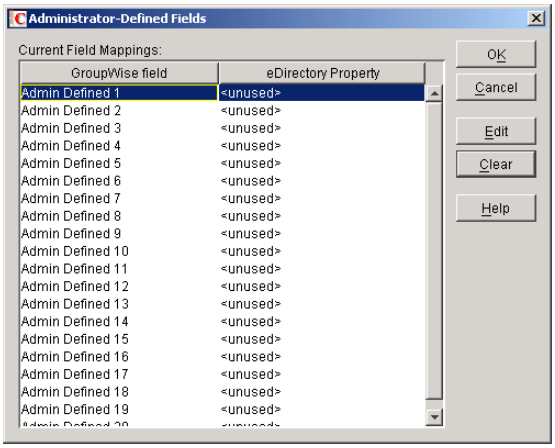
For user information to be displayed in the GroupWise Address Book, it must be stored not only in eDirectory but also in the GroupWise domain and post office databases. If you add or modify user information using an installation of ConsoleOne with the GroupWise Administrator snap-in, the GroupWise Administrator snap-in adds the user information to the GroupWise databases. However, if you add or modify user information using a ConsoleOne installation that is not running the GroupWise Administrator snap-in, the user information is not changed in the GroupWise databases. This is also true if you add or modify user information using NetWare Administrator, NETADMIN, or NWDS API.

To ensure that the user information stored in the GroupWise databases is always synchronized with the user information in eDirectory, you can set up eDirectory user synchronization. For detailed information see "Using eDirectory User Synchronization" on page 598.

Admin-Defined Fields

eDirectory includes user information that is not associated to GroupWise user fields. For example, a User object includes Postal Address fields named "City," "State," and "Zip Code." By default, these fields are not included as GroupWise fields. However, you can use the Admin-Defined Fields feature to map eDirectory user fields to GroupWise fields so that they can be displayed in the GroupWise Address Book.

1 In ConsoleOne, click the Tools menu > GroupWise System Operations > Admin-Defined Fields to display the Administrator-Defined Fields dialog box.

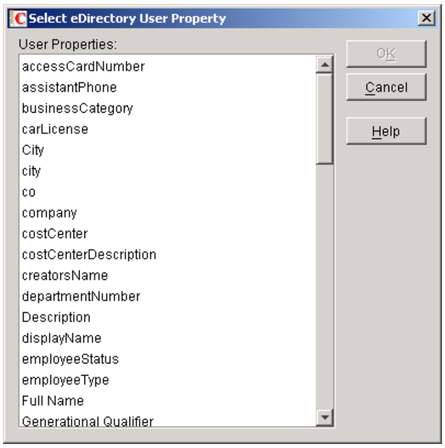


Administrator-Defined Fields

Current Field Mappings:

GroupWise field	eDirectory Property
Admin Defined 1	<unused>
Admin Defined 2	<unused>
Admin Defined 3	<unused>
Admin Defined 4	<unused>
Admin Defined 5	<unused>
Admin Defined 6	<unused>
Admin Defined 7	<unused>
Admin Defined 8	<unused>
Admin Defined 9	<unused>
Admin Defined 10	<unused>
Admin Defined 11	<unused>
Admin Defined 12	<unused>
Admin Defined 13	<unused>
Admin Defined 14	<unused>
Admin Defined 15	<unused>
Admin Defined 16	<unused>
Admin Defined 17	<unused>
Admin Defined 18	<unused>
Admin Defined 19	<unused>
Admin Defined 20	<unused>

2 Select an Admin-definable field (for example, Admin Defined 1), then click Edit to display the Select eDirectory User Property dialog box.



Select eDirectory User Property

User Properties:

accessCardNumber
assistantPhone
businessCategory
carLicense
City
city
co
company
costCenter
costCenterDescription
creatorsName
departmentNumber
Description
displayName
employeeStatus
employeeType
Full Name
Generational Qualifier

3. Select the eDirectory user property that you want to map to the GroupWise field, then click OK to create the mapping.
4. Repeat Step 2 and Step 3 to map additional fields.
5. When finished, click OK to close the Administrator-Defined Fields dialog box.
6. To use the field in the GroupWise Address Book, see "Determining Fields, Field Order, and Sort Order for the Address Book" on page 81.

Pending Operations

Pending operations are the results of administrative operations, such as adding GroupWise objects and modifying GroupWise object properties, that have not yet been permanently written to the appropriate GroupWise databases. While operations are pending, GroupWise data is not in a stable, consistent state.

For example, you can maintain any domain's objects you have administrative rights over. However, because a secondary domain owns its own objects, any operation you perform from the primary domain on a secondary domain's objects must be validated by the secondary domain. While the operation is being validated, the Pending Operations dialog box displays object details and the pending operation.

While the operation is pending, the object is marked Unsafe in the primary domain database. The Operation field in the dialog box displays the pending operation. An unsafe object can have other operations performed on it, such as being added to a distribution list; however, the object record is not distributed to other domains and post offices in the system until it is marked Safe.

All pending operations require confirmation that the operation was either successfully performed or could not be performed. If the operation was successful, the pending operation is removed from the list, the record is marked in the database as Safe, and the record is distributed to all other domains and post offices in your system. If the operation could not be performed, the pending operation remains in the list where you can monitor and manage it.

- "Viewing Pending Operations" on page 51
- "Retrying a Pending Operation" on page 51
- "Cancelling a Pending Operation" on page 52

Viewing Pending Operations

1. In ConsoleOne, connect to the domain whose pending operations you want to view (see "Select Domain" on page 43), then click the Tools menu > GroupWise System Operations > Pending Operations.

   While an operation is being validated, the Pending Operations dialog box displays the object and the operation waiting completion and confirmation.
2. For more detailed information, select the pending operation, then click View.

Retrying a Pending Operation

1. Make sure the agents are running for the domain and/or post office where the operation must take place.
2. In the Pending Operations dialog box, select the pending operation, then click Retry.

Cancelling a Pending Operation

1 In the Pending Operations dialog box, select the pending operation, then click Undo.

Addressing Rules

You can use the Addressing Rules feature to configure GroupWise so that users can enter shortened forms of e-mail addresses. For more information, see Chapter , "Addressing Rules," on page 97.

Time Zones

When you create a domain or post office, you select the time zone in which it is located. This ensures that GroupWise users in other time zones receive Calendar events and tracking information adjusted for local time.

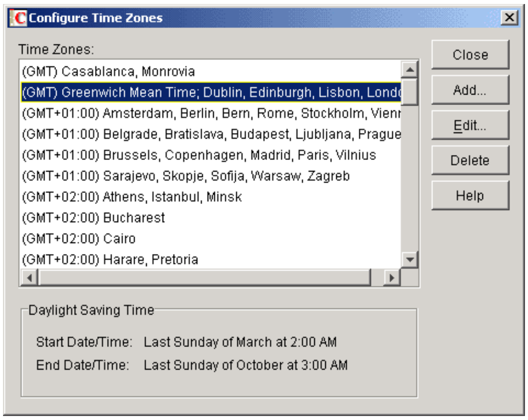
The time zone list includes predefined definitions for each time zone. Most time zones include multiple definitions to account for different locations within the time zone. Each time zone definition allows you to specify the Daylight Saving Time dates and bias (1 hour, 30 minutes, etc.).

You can modify existing time zone definitions, add new definitions, or delete definitions.

- "Modifying a Time Zone Definition" on page 52
- "Adding a Time Zone Definition" on page 53
- "Deleting a Time Zone Definition" on page 55

Modifying a Time Zone Definition

1 In ConsoleOne, click the Tools menu > GroupWise System Operations > Time Zones.



Configure Time Zones

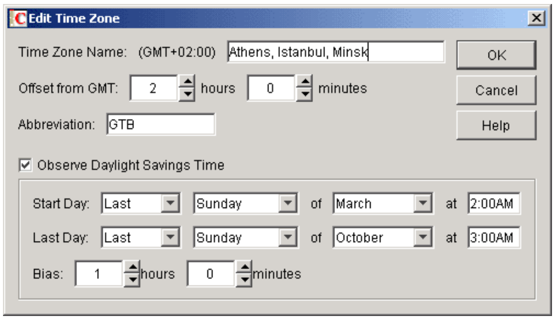
Time Zones:

(GMT) Casablanca, Monrovia
(GMT) Greenwich Mean Time; Dublin, Edinburgh, Lisbon, Lond
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vien
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris, Vilnius
(GMT+01:00) Sarajevo, Skopje, Sofija, Warsaw, Zagreb
(GMT+02:00) Athens, Istanbul, Minsk
(GMT+02:00) Bucharest
(GMT+02:00) Cairo
(GMT+02:00) Harare, Pretoria

Daylight Saving Time

Start Date/Time: Last Sunday of March at 2:00 AM
End Date/Time: Last Sunday of October at 3:00 AM

2 Select the time zone to modify, then click Edit to display the Edit Time Zone dialog box.



Time Zone Name: (GMT+02:00) Athens, Istanbul, Minsk

Offset from GMT: 2 hours 0 minutes

Abbreviation: GTB

☑ Observe Daylight Savings Time

Start Day: Last Sunday of March at 2:00AM

Last Day: Last Sunday of October at 3:00AM

Bias: 1 hours 0 minutes

3 Modify any of the following fields:

Time Zone Name: Provide a name for the time zone definition (for example, some of the major cities in the time zone). We suggest you include a reference (+ or -) to GMT, for example (GMT-07:00). The time zone list is sorted by the GMT offset.

Offset from GMT: Enter the hours and minutes that the time zone is offset from Greenwich Mean Time. The offset from GMT keeps your different locations synchronized. For example, if a conference call is scheduled for 4:00 p.m. June 1 in Salt Lake City, the call would appear on a schedule in Adelaide at 8:30 a.m. June 2. If you are in the western hemisphere (west of the Greenwich Meridian and east of the International Date Line) be sure the hour offset is negative (-). If you are in the eastern hemisphere (east of the Greenwich meridian and west of the International Date Line) be sure the hour offset is positive.

Abbreviation: Enter an abbreviation for the time zone. For example, the abbreviation for Atlantic Standard Time could be AST; the abbreviation for Atlantic Daylight Time could be ADT.

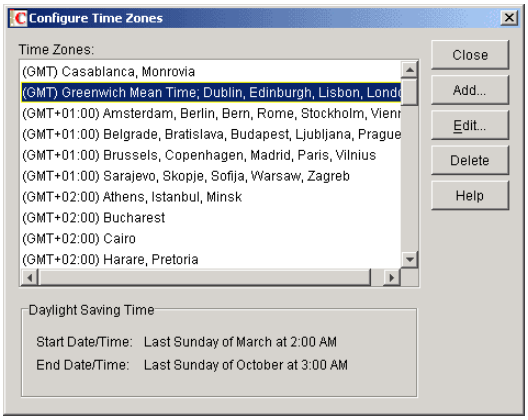
Observe Daylight Saving Time: If the time zone observes daylight saving time, click the Observe Daylight Saving Time box, then fill out the remaining fields:

- Start Day: Select the day and time that daylight saving time starts.
- Last Day: Select the day and time that daylight saving time ends.
- Bias: Select the number of hours and minutes that the clock changes at the daylight saving time start day, such as1 hour or 1 hour 30 minutes.

4 Click OK to save the changes.

Adding a Time Zone Definition

1 In ConsoleOne, click the Tools menu > GroupWise System Operations > click Time Zones.



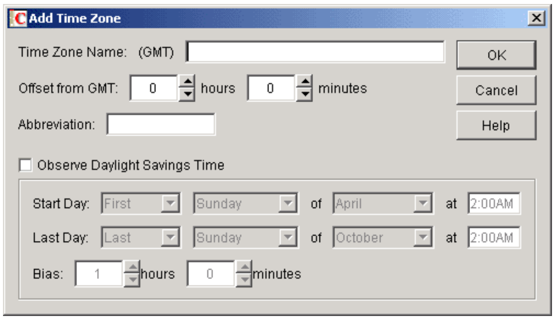
Time Zones:

(GMT) Casablanca, Monrovia
(GMT) Greenwich Mean Time; Dublin, Edinburgh, Lisbon, Londo
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienr
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris, Vilnius
(GMT+01:00) Sarajevo, Skopje, Sofija, Warsaw, Zagreb
(GMT+02:00) Athens, Istanbul, Minsk
(GMT+02:00) Bucharest
(GMT+02:00) Cairo
(GMT+02:00) Harare, Pretoria

Daylight Saving Time

Start Date/Time: Last Sunday of March at 2:00 AM
End Date/Time: Last Sunday of October at 3:00 AM

2 Click Add to display the Add Time Zone dialog box.



Time Zone Name: (GMT)

Offset from GMT: 0 hours 0 minutes

Abbreviation:

□ Observe Daylight Savings Time

Start Day: First Sunday of April at 2:00AM

Last Day: Last Sunday of October at 2:00AM

Bias: 1 hours 0 minutes

3 Fill in the following fields:

Time Zone Name: Provide a name for the time zone definition (for example, some of the major cities in the time zone). We suggest you include a reference (+ or -) to GMT, for example (GMT-07:00). The time zone list is sorted by the GMT offset.

Offset from GMT: Enter the hours and minutes that the time zone is offset from Greenwich Mean Time. The offset from GMT keeps your different locations synchronized. For example, if a conference call is scheduled for 4:00 p.m. June 1 in Salt Lake City, the call would appear on a schedule in Adelaide at 8:30 a.m. June 2. If you are in the western hemisphere (west of the Greenwich Meridian and east of the International Date Line) be sure the hour offset is negative (-). If you are in the eastern hemisphere (east of the Greenwich meridian and west of the International Date Line) be sure the hour offset is positive.

Abbreviation: Enter an abbreviation for the time zone. For example, the abbreviation for Atlantic Standard Time could be AST; the abbreviation for Atlantic Daylight Time could be ADT.

Observe Daylight Saving Time: If the time zone observes daylight saving time, click the Observe Daylight Saving Time box, then fill out the remaining fields:

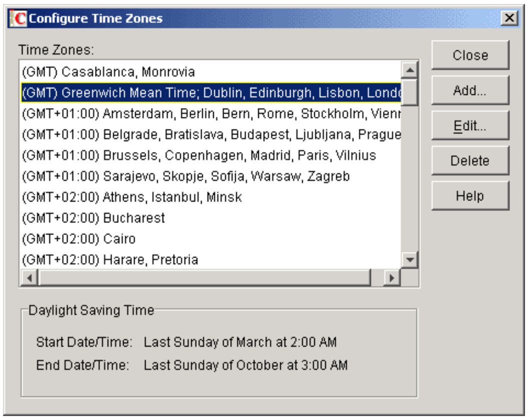
- Start Day: Select the day and time that daylight saving time starts.
- Last Day: Select the day and time that daylight saving time ends.
- Bias: Select the number of hours and minutes that the clock changes at the daylight saving time start day, such as1 hour or 1 hour 30 minutes.

4 Click OK to add the definition to the time zone list.

Deleting a Time Zone Definition

When you delete a time zone from the list, you can no longer select it for a domain or post office. To delete a time zone:

1. In ConsoleOne, click the Tools menu > GroupWise System Operations > Time Zones.



Time Zones:

(GMT) Casablanca, Monrovia
(GMT) Greenwich Mean Time; Dublin, Edinburgh, Lisbon, Londo
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienr
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris, Vilnius
(GMT+01:00) Sarajevo, Skopje, Sofija, Warsaw, Zagreb
(GMT+02:00) Athens, Istanbul, Minsk
(GMT+02:00) Bucharest
(GMT+02:00) Cairo
(GMT+02:00) Harare, Pretoria

Daylight Saving Time

Start Date/Time: Last Sunday of March at 2:00 AM
End Date/Time: Last Sunday of October at 3:00 AM

2. Select the time zone to remove from the list, click Delete, then click Yes to confirm the deletion.

External System Synchronization

The External System Synchronization feature lets you automatically synchronize information between your system and an external GroupWise system connected to your system (for information about connecting GroupWise systems, see "Connecting to GroupWise 5.x and 6.x Systems" in the *GroupWise 6.5 Multi-System Administration Guide*). This simplifies message addressing by enabling your users to select the other system's users from the Address Book. Otherwise, your users are required to enter the recipient's full address (*userID.post_office.domain* or *user@host*).

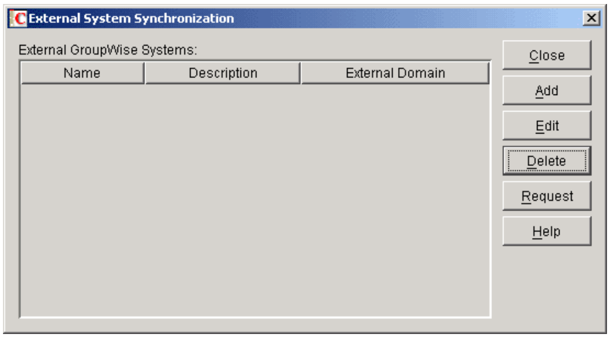
IMPORTANT: The External System Synchronization feature exists in GroupWise 5.*x* and 6.*x* only. Therefore, you can use it to synchronize information between 5.*x* and 6.*x* systems only. You cannot use it to synchronize information between 6.*x* and 4.*x* or 3.*x* systems.

External System Synchronization lets you control what information (domains, post offices, users, resources, and distribution lists) you send to the external system and what information you want to accept from the external system. Any user, resource, and distribution list information you receive from the external GroupWise system is displayed in the system Address Book.

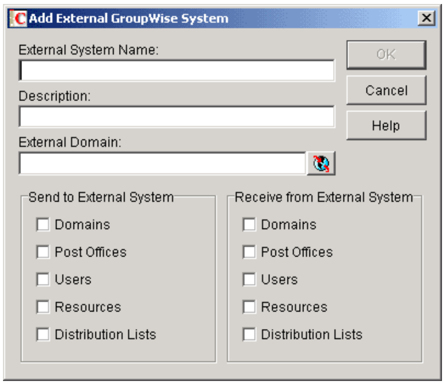
External synchronization must be set up in both GroupWise systems before it can work properly.

To set up synchronization so that all future Address Book changes are propagated to external GroupWise systems:

1. In ConsoleOne, click the Tools menu > GroupWise System Operations > External System Synchronization to display the External System Synchronization dialog box.



2 Click Add to display the Add External GroupWise System dialog box.



3 Fill in the following fields:

External System Name: Enter the name of the external GroupWise system. The name needs to match the actual name of that GroupWise system.

Description: If desired, enter a description for the external system. This is an optional field.

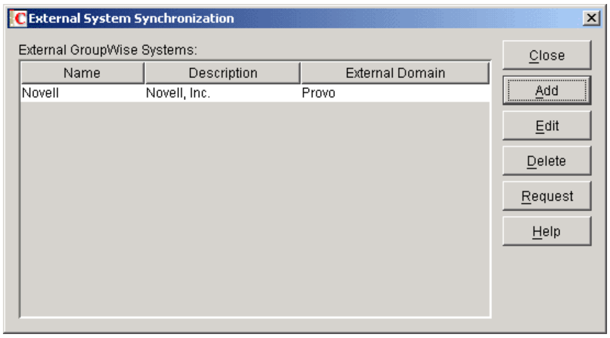
External Domain: Click the External Domain (globe) icon to display a list of the external domains defined in your GroupWise system. Select the external domain that belongs to the external GroupWise system with which you are synchronizing information.

Send to External System: Select the information (Domains, Post Offices, Users, Resources, and Distribution Lists) you want sent to the external GroupWise system during synchronization. Only the information that your system owns is sent. For example, if you've connected to another GroupWise system and its information is contained in your GroupWise system as external domains, post offices, users, resources, and distribution lists, that information is not sent.

A user, resource, or distribution list from your system is added to the external GroupWise system only if its domain and post office exist in the external system (as an external domain and post office in that system). Because of this, you'll want to make sure that the Domains and Post Offices options are selected as well as the desired Users, Resources, and Distribution Lists options. After the initial synchronization takes place, the domains and post offices exist in the external system. You can then choose not to send domain and post office information. However, if you add domains or post offices or change the information for your existing domains and post offices, that information is not sent to the external system until you select Domains and Post Offices again.

Receive from External System: Select the information (Domains, Post Offices, Users, Resources, and Distribution Lists) you are willing to receive from the external GroupWise system. As with sending information, a user, resource, or distribution list is added to your system only if its domain and post office exist as an external domain and post office in your system. Therefore, you should make sure to select the Domains and Post Offices options for at least the initial synchronization.

4 Click OK to add the external GroupWise system to the list of external systems you are synchronizing information with.



Name	Description	External Domain
Novell	Novell, Inc.	Provo

5 Click Close to save your changes.

After External System Synchronization is configured in both GroupWise systems, the two systems exchange information. After the initial synchronization, any time domain, post office, user, resource, or distribution list information in one system changes, the new information is sent to the other system (provided that information is flagged to be sent).

Software Directory Management

The Software Directory Management feature lets you manage GroupWise software distribution directories. A software distribution directory is simply an image of the *GroupWise 6.5* CDs located on a network server. From this network location, you can distribute the GroupWise client software to users or install additional GroupWise software such as the Message Transfer Agent, Post Office Agent, Internet Agent, WebAccess, and Monitor.

When you install GroupWise, one software distribution directory is created automatically. Using Software Directory Management, you can create new software distribution directories, update existing software distribution directories, or delete existing software distribution directories.

- "Creating a Software Distribution Directory" on page 57
- "Updating a Software Distribution Directory" on page 59
- "Deleting a Software Distribution Directory" on page 60

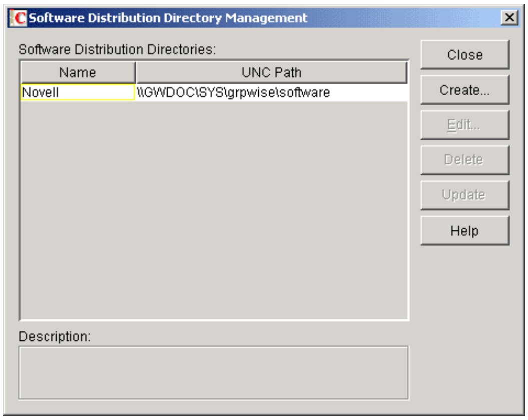
To view the structure and contents of a software distribution directory, see "Software Distribution Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Creating a Software Distribution Directory

1 Make sure the directory you want to use as the software distribution directory exists.

All distribution subdirectories (\admin, \agents, \client, and so forth) will be created under this directory.

2 Click the Tools menu > GroupWise System Operations > Software Directory Management to display the Software Distribution Directory Management dialog box.


Software Distribution Directory Management

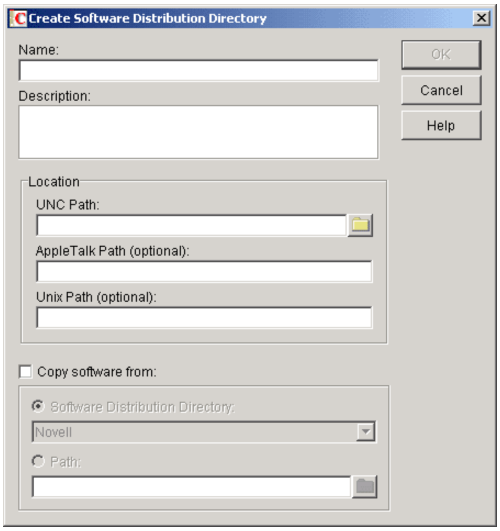
Software Distribution Directories:

Name	UNC Path
Novell	\\GWDOC\SYS\grpwise\software

Description:

The Software Distribution Directories list includes all software distribution directories defined in your GroupWise system.

3 Click Create to display the Create Software Distribution Directory dialog box.


Create Software Distribution Directory

Name:

Description:

Location

UNC Path:

AppleTalk Path (optional):

Unix Path (optional):

□ Copy software from:

● Software Distribution Directory: Novell

○ Path:

4 Fill in the following fields:

Name: Enter a name to identify the software distribution directory within your GroupWise system. For example, whenever you create a post office, you associate it with a software distribution directory. The software distribution directory's name, not its location, appears in the list of directories from which you can select. The name can include any characters; there are no restrictions.

Description: Enter an optional description for the software distribution directory. You might want to use this description to indicate the software version or to give other pertinent information.

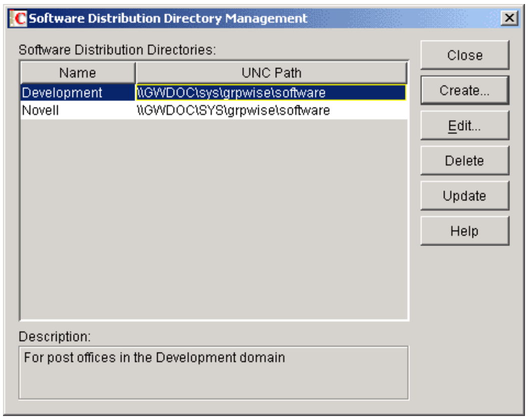
Location: In the UNC Path field, enter the location where you want to create the software distribution directory. If you specify a path to a directory that does not exist, ConsoleOne creates the directory for you. The UNC path is also used by GroupWise software (running on Windows* workstations) to locate the software distribution directory when necessary. If you have GroupWise software running on Macintosh* or UNIX* workstations, you can use the optional AppleTalk* Path and UNIX Path fields to specify the directory location from the perspective of the Macintosh and UNIX workstations.

NOTE: On Linux, a Linux Path field is provided instead of the UNIX Path field for use by the GroupWise Cross-Platform client on Linux.

Copy Software From: Select this option to copy GroupWise software to the new directory, then choose from the following source locations:

- Software Distribution Directory: If you want to copy software from an existing software distribution directory, select this option, then select the software distribution directory. All directories are copied.
- Path: If you want to copy software from a location, such as the *GroupWise 6.5* CDs, that is not defined as a software distribution directory in your GroupWise system, select this option, then browse for and select the correct path.

5 Click OK to create the software distribution directory and add it to the list.



Software Distribution Directories:

Name	UNC Path
Development	\\GWDOC\sys\grpwise\software
Novell	\\GWDOC\SYS\grpwise\software

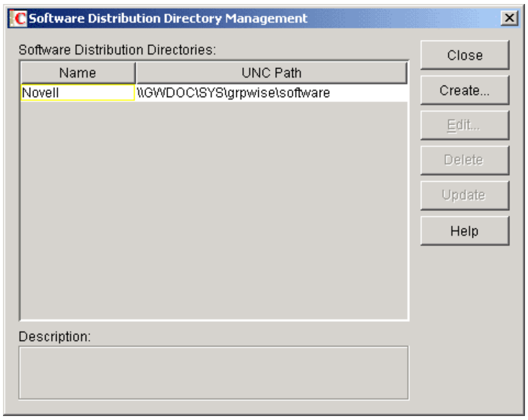
Description:

For post offices in the Development domain

6 Click Close to exit the dialog box.

Updating a Software Distribution Directory

1 Click the Tools menu > GroupWise System Operations > Software Directory Management to display the Software Distribution Directory Management dialog box.



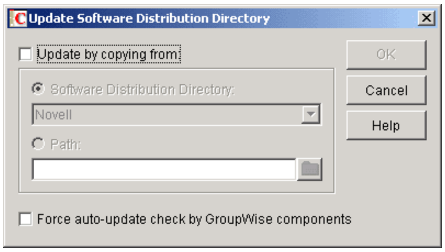
Software Distribution Directories:

Name	UNC Path
Novell	\\GWDOC\SYS\grpwise\software

Description:

The Software Distribution Directories list includes all software distribution directories defined in your GroupWise system.

2 Select the software distribution directory to update, then click Update to display the Update Software Distribution Directory dialog box.



□ Update by copying from:

● Software Distribution Directory: Novell

○ Path:

□ Force auto-update check by GroupWise components

3 Fill in the following fields:

Update by Copying From: Select this option, then choose from the following source locations:

- Software Distribution Directory: If you want to copy software from an existing software distribution directory, select this option, then select the software distribution directory. All files and subdirectories are copied.
- Path: If you want to copy software from a location, such as the *GroupWise 6.5* CDs, that is not defined as a software distribution directory in your GroupWise system, select this option, then browse for and select the correct path.

Force Auto-Update Check by GroupWise Components: This option causes the GroupWise Post Office Agent (in client/server access mode) or the GroupWise client (in direct access mode) to check the software distribution directory for a new version of the GroupWise client; if a new version is found, the next time a user starts the GroupWise client, he or she is prompted to update the client software.

The Force Auto-Update Check by GroupWise Components option is automatically selected when you select the Update by Copying From option. If you don't select the Update by Copying From option, you can still select this option and then click OK. This forces an auto-update check of the client software version, but the software distribution directory's files are not updated.

To determine the current client software version in ConsoleOne, click Tools > GroupWise Diagnostics > Record Enumerations to display a list of records types in the domain database. From the drop-down list, select Areas by ID, select a software distribution directory, then click Info to list detailed information about the software distribution directory. Check the Software Version field to determine the GroupWise client software version.

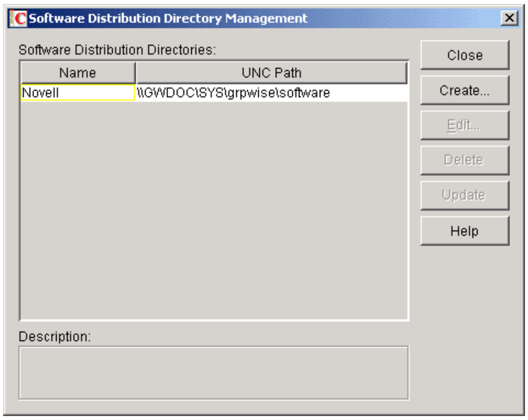
4 Click OK to update the directory's software.

Deleting a Software Distribution Directory

When you delete a software distribution directory, the directory is removed from the file system and no longer appears in the list of software distribution directories. Any post office that was assigned to that software distribution directory defaults to the first directory in the list.

To delete a software distribution directory:

1 Click the Tools menu > GroupWise System Operations > Software Directory Management to display the Software Distribution Directory Management dialog box.



Software Distribution Directories:

Name	UNC Path
Novell	\\GWDOC\SYS\grpwise\software

Description:

The Software Distribution Directories list includes all software distribution directories defined in your GroupWise system.

2 Select the directory to delete, click Delete, then click Yes to confirm the deletion.

Restore Area Management

A restore area is a location you designate to hold a backup copy of a post office so that you or GroupWise client users can access it to retrieve mailbox items that are unavailable in your live GroupWise system. The Restore Area Management feature lets you manage your GroupWise system's restore areas.

Detailed information for using restore areas is provided in "Restoring Deleted Mailbox Items" on page 381. Information about backing up post offices is provided in "Backing Up a Post Office" on page 375.

Internet Addressing

By default, GroupWise uses a proprietary address format consisting of a user's ID, post office, and domain (*userID.post_office.domain*). However, if you have the GroupWise Internet Agent installed (see "Internet Agent" on page 659), GroupWise also supports native Internet-style addressing consisting of a username and Internet domain name (*username@Internet_domain_name*).

You use the Internet Addressing feature to do the following:

- Define Internet domain names for your GroupWise system. You can have one or more domain names (for example, novell.com, gw.novell.com, and support.novell.com).
- Set up the default Internet address format for use when displaying user addresses in the GroupWise Address Book and sent messages. There are six formats that can be assigned at the system, domain, post office, or user level. In addition, there is a free-form format that can be used at the user level.
- Designate the address formats that can be used to address messages to your GroupWise users. There are five possible formats to choose from. You can allow all five formats, or only one.
- Specify the default Internet Agent to be used when sending messages from your GroupWise system to the Internet. This becomes your system's default Internet Agent for outbound messages sent from all domains; however, if you have multiple Internet Agents, you can override this setting by assigning Internet Agents at the domain level.

For detailed information about Internet addressing, see Chapter , "Internet-Style Addressing," on page 87.

Trusted Applications

Trusted applications are third-party programs that can log into Post Office Agents (POAs) in order to access GroupWise mailboxes. Trusted applications might perform such services as virus scanning or content filtering within your GroupWise system, relying on Message Transfer Agents (MTAs) for message transport. The Trusted Application feature allows you to edit and delete trusted applications that are available in your GroupWise system.

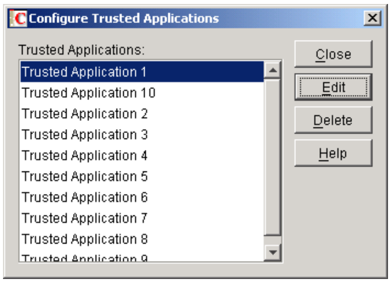
For information about creating and installing trusted applications, search for *GroupWise Trusted Application API* at the Novell Developer Kit (NDK) Web site (http://developer.novell.com/ndk).

- "Editing a Trusted Application" on page 62
- "Deleting a Trusted Application" on page 63

Editing a Trusted Application

You can edit a trusted application's description, IP address, port, and SSL settings.

1 Click the Tools menu > GroupWise System Operations > Trusted Applications to display the Configure Trusted Applications dialog box.

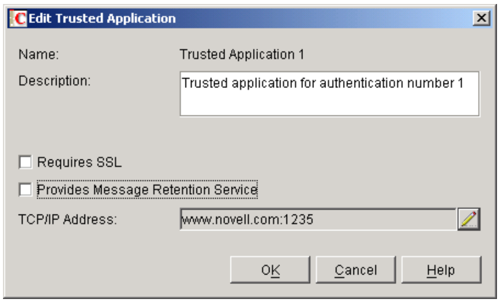


Configure Trusted Applications

Trusted Applications:

Trusted Application 1
Trusted Application 10
Trusted Application 2
Trusted Application 3
Trusted Application 4
Trusted Application 5
Trusted Application 6
Trusted Application 7
Trusted Application 8
Trusted Application 9

2 In the Trusted Applications list, select the application you want to edit, then click Edit.



Edit Trusted Application

Name: Trusted Application 1

Description: Trusted application for authentication number 1

□ Requires SSL

□ Provides Message Retention Service

TCP/IP Address: www.novell.com:1235

3 Modify any of the following fields:

Name: This field displays the trusted application's name. You cannot change the name.

Description: Enter a description for the trusted application.

Requires SSL: Select this option to require a secure (SSL) connection between the trusted application and MTAs or POAs.

Provides Message Retention Service: Select this option if the purpose of the trusted application is to retain GroupWise user messages by copying them from GroupWise mailboxes (user databases) into another storage medium.

Turning on this option only defines the trusted application as a Message Retention Service application. In order for GroupWise mailboxes to support message retention, you must turn on the Enable Message Retention Service option in the GroupWise Client Options (Tools menu> GroupWise Utilities> Client Options > Environment > Retention). You can enable individual mailboxes, all mailboxes in a post office, or all mailboxes in a domain by selecting the appropriate object (User, Post Office, or Domain) before selecting GroupWise Client Options. For more information, see Chapter 74, "Setting Defaults for the GroupWise Client Options," on page 973.

For information about the complete process required to use a trusted application for message retention, see Chapter 33, "Retaining User Messages," on page 387.

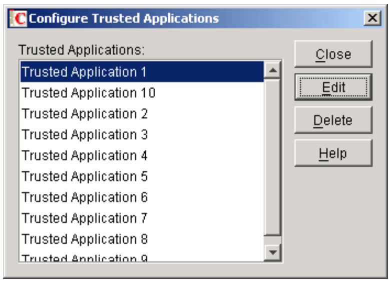
TCP/IP Address: If you want to restrict the location from which the trusted application can run, enter the IP address of the server from which the application can run. To do so, click the Edit (pencil) button, then enter the IP address or DNS hostname of the trusted application's server.

If you want to allow the trusted application to be run from any server, do not enter an IP address or DNS hostname.

For information about how the POA handles trusted application processing of message files, see "Configuring Trusted Application Support" on page 466.

Deleting a Trusted Application

1 Click the Tools menu > GroupWise System Operations > Trusted Applications to display the Configure Trusted Applications dialog box.



Trusted Application 1
Trusted Application 10
Trusted Application 2
Trusted Application 3
Trusted Application 4
Trusted Application 5
Trusted Application 6
Trusted Application 7
Trusted Application 8
Trusted Application 9

2 In the Trusted Applications list, select the application you want to delete, click Delete, then click Yes to confirm the deletion.

LDAP Servers

The LDAP Servers feature lets you define the LDAP servers you want used for LDAP authentication to GroupWise mailboxes.

For information about defining LDAP servers, see "Providing LDAP Server Configuration Information" on page 461.

For information about using LDAP for user authentication to GroupWise mailboxes, see "Providing LDAP Authentication for GroupWise Users" on page 461.

5 GroupWise Utilities

The GroupWise® utilities in ConsoleOne® are used to perform various maintenance and configuration tasks for your GroupWise system. The following sections provide information about the system utilities included on the Tools menu (Tools menu > GroupWise System Utilities):

- "Mailbox/Library Maintenance" on page 66
- "System Maintenance" on page 66
- "Backup/Restore Mailbox" on page 66
- "Recover Deleted Account" on page 66
- "Client Options" on page 66
- "Expired Records" on page 67
- "Email Address Lookup" on page 67
- "Synchronize" on page 67
- "User Move Status" on page 68
- "Link Configuration" on page 68
- "Document Properties Maintenance" on page 68
- "Import" on page 68
- "Export" on page 71
- "New System" on page 72
- "GW / eDirectory Association" on page 73

In addition to the system utilities included on the Tools menu in ConsoleOne, GroupWise includes the following standalone utilities:

- "GroupWise Check Utility (GWCheck)" on page 78
- "GroupWise Target Service Agent (GWTSA)" on page 78
- "GroupWise Backup Time Stamp Utility (GWTMSTMP)" on page 78
- "GroupWise Database Copy Utility (DBCOPY)" on page 78
- "GroupWise Generate CSR Utility (GWCSRGEN)" on page 79

Mailbox/Library Maintenance

You can use the Mailbox/Library Maintenance utility to check the integrity of and repair user/resource, message, and library databases, and to free disk space in post offices.

For detailed information and instructions, see Chapter 27, "Maintaining User/Resource and Message Databases," on page 353, Chapter 28, "Maintaining Library Databases and Documents," on page 359, and Chapter 30, "Managing Database Disk Space," on page 367.

System Maintenance

You can use the System Maintenance utility to check the integrity of and repair domain and post office databases.

For detailed information and instructions, see Chapter 26, "Maintaining Domain and Post Office Databases," on page 345.

Backup/Restore Mailbox

You can use the Backup/Restore Mailbox utility to restore an individual user's Mailbox items from a backup copy of the post office database.

For detailed information and instructions, see Chapter 32, "Restoring GroupWise Databases from Backup," on page 379.

Recover Deleted Account

If you have a reliable backup procedure in place, you can use the Recover Deleted Account utility to restore recently deleted user and resource accounts from the backup version of the GroupWise primary domain database. After the account has been re-created, you can then restore the corresponding mailbox and its contents to complete the process. Membership in distribution lists and ownership of resources must be manually re-established.

For complete instructions, see "Recovering Deleted GroupWise Accounts" on page 384.

Client Options

You can use the Client Options utility to set the default options (preferences) for the GroupWise client. You can set options at the domain, post office, or user level. Options set at the domain level apply to all users in the domain, and options set at the post office level apply to all users in the post office. If you don't want users to change options, you can lock the options.

NOTE: The GroupWise Cross-Platform client does not yet support all of the client options that can be set in ConsoleOne.

For detailed information and instructions, see Chapter 74, "Setting Defaults for the GroupWise Client Options," on page 973.

Expired Records

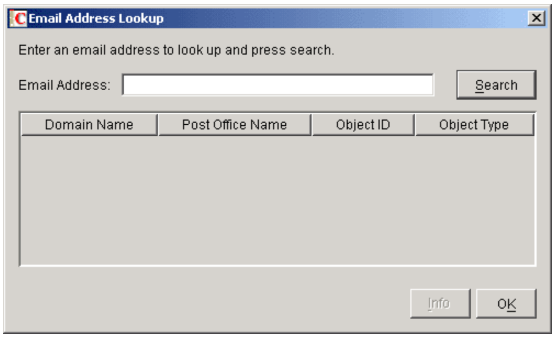
You can use the Expired Records utility to view and manage the GroupWise user accounts that have an expiration date assigned to them.

For detailed information and instructions, see Chapter , “Removing GroupWise Accounts,” on page 215.

Email Address Lookup

You can use the Email Address Lookup utility to search for the GroupWise object (User, Resource, Distribution List) that an e-mail address is associated with. You can then view the object’s information.

1 In ConsoleOne, click the Tools menu > GroupWise Utilities > Email Address Lookup to display the Email Address Lookup dialog box.



Enter an email address to look up and press search.

2 In the Email Address field, enter the e-mail address. You can enter the username only (for example, jsmith) or the entire address (for example, jsmith@novell.com).

3 Click Search.

All objects whose e-mail address match the one you entered are displayed.

4 If desired, select an object, then click Info to see details about the object.

Synchronize

GroupWise automatically replicates information (domain, post office, user, resource, and so forth) to all domain and post office databases throughout your GroupWise system. This ensures that the information in each database is synchronized.

Situations might occur, however, that result in information not being replicated to all domain and post office databases. If you think that some information has not been replicated correctly, you can cause the information to be replicated again so that it becomes synchronized throughout your entire GroupWise system. For example, if you notice that a user’s information is incorrect in the Address Book, you can synchronize that user’s eDirectory User object so that his or her information is replicated to all domain and post office databases again.

For detailed information and instructions, see Chapter 29, “Synchronizing Database Information,” on page 363.

User Move Status

You can use the User Move Status utility to track progress as you move users from one post office to another. Using the User Move Status utility, you can:

- List users that are currently being moved and filter the list by domain, post office, and object.
- View the current status of the move for each object and see any errors that have occurred.
- Immediately retry a move where some of the information on the user inventory list failed to arrive at the destination post office. By default, the POA retries automatically every 12 hours for seven days to move all the information included on the user inventory list.
- Stop the POA from continuing its automatic retries.
- Restart (from the beginning) a move that has stopped before successful completion.
- Refresh the list to display current move status and clear completed moves from the list.

For more information, see "Monitoring User Move Status" on page 203.

Link Configuration

GroupWise domains and post offices must be properly linked in order for messages to flow throughout your GroupWise system. You can use the Link Configuration utility to ensure that your domains and post offices are properly linked and to optimize the links if necessary. For detailed information and instructions, see Chapter 10, "Managing the Links between Domains and Post Offices," on page 131.

Document Properties Maintenance

Each document stored in the GroupWise Document Management Services (DMS) has properties associated with it. These properties identify the document, determine its disposition (archive, delete, keep), set its level of security, and provide information for locating it in searches. Certain document properties are standard in GroupWise. You can also customize DMS for your organization by defining additional properties. For detailed information and instructions, see "Customizing Document Properties" on page 306.

NOTE: On Linux, Document properties maintenance is not available in ConsoleOne.

Import

The GroupWise Import utility reads an ASCII-delimited text file created by the GroupWise Export utility or by a third-party export, and creates Novell® eDirectory™ and GroupWise objects with attributes from the file. The Import utility supports most eDirectory classes (including extensions) and GroupWise classes. You can specify the delimiters, eDirectory contexts, and file field positions to use during import.

An important use of the Import utility is to give GroupWise accounts to new or existing eDirectory users.

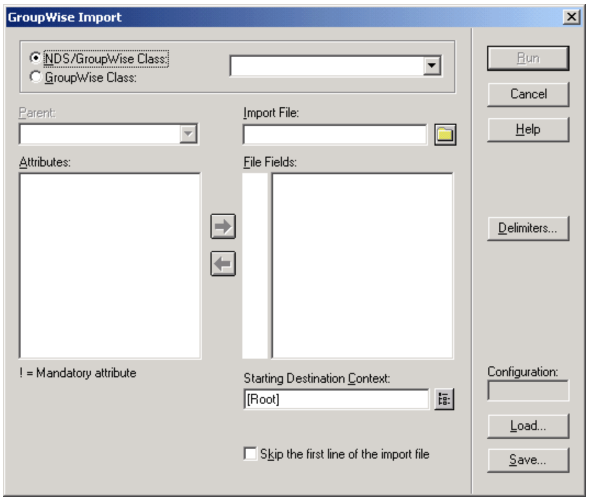
IMPORTANT: The Import utility is not included on the *GroupWise 6.5* CDs. You can download the Import/Export utility from TID 2960897 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp). To install the Import/Export utility, follow the instructions provided with the download. The Import/Export utility is not available for use on Linux.

To import objects into GroupWise, the following conditions must be met:

- You must create an ASCII-delimited text file by using the GroupWise Export utility or another export utility.
- The destination context for each eDirectory object must already exist. The GroupWise Import utility supports creating organizational units. If a large portion of a tree needs to be reconstructed to support the objects, you can import organizational units before importing the objects.

To import objects into GroupWise:

1 In ConsoleOne, select the eDirectory tree to which the objects will be imported, click the Tools menu > GroupWise Utilities > Import to display the GroupWise Import dialog box.



Starting Destination Context: [Root]

2 If you have previously defined and saved a configuration file, click Load to fill in the fields from the configuration files, then click Run to perform the import.

or

Fill in the fields in the Import Dialog box.

NDS/GroupWise Class: Select this option to import objects belonging to an eDirectory class or to a GroupWise-related eDirectory class. Choose the class from the list.

GroupWise Class: Select this option to import objects belonging to a GroupWise class not represented in eDirectory. Choose external user, external domain, external post office, Document-Version, or Lookup Entry from the list

Parent: If you are importing objects that belong to a GroupWise-related eDirectory class or a GroupWise-only class, the parent attribute is required unless:

- The class is the eDirectory User class, in which case the object can be optionally associated with GroupWise by specifying a value here.
- The value is in the import file and is explicitly imported by your positioning the NGW: Post Office attribute in the File Fields list box, explained below. In this case, if the value obtained from the file is blank, the Post Office field value, if any, is used.

Import File: Specify the full path and file name of the ASCII text file.

Attributes / File Fields: This list displays the attributes of the selected class. Move the attributes to correspond to the fields in the ASCII text file to the File Fields list.

Some attributes are marked with an exclamation point (!), indicating that a value for that attribute must exist for a successful import. The import also requires a value for either the object name or distinguished name.

Starting Destination Context: Specify the destination eDirectory context for the objects to be imported. If DN or Context from Root is selected as an import field, the value in this field is ignored because both DN and Context from Root specify the destination context.

An imported object's position in the tree can be constructed in a flexible manner using the Context from Root, Context from Starting, DN, and Object Name class attribute fields and the Starting Destination Context field. The following combinations are valid:

DN	Each object's name and context are found in this field value.
Object Name + Starting Destination Context	Each object name in the Object Name field is added to the context entered in Starting Destination Context.
Object Name + Context from Starting + Starting Destination Context	Each object name in the Object Name field is added to the context obtained by concatenating the value in the Context from Starting field and the value entered in Starting Destination Context.
Object Name + Context from Root	Each object name in the Object Name field is added to the context read from the Context from Root field.

Skip the First Line of the Import File: This directs the import to skip the first line if it contains the attribute names.

Delimiters: Accept the defaults shown or change the delimiters to match those used by the export file. For more information, see "Delimiters" on page 70.

3 For convenience, save the configuration for later user. See "Loading or Saving a Configuration File" on page 70.

4 Click Run to perform the import.

An import.log file is created in the same directory as the import file and contains a list of the imported objects.

Loading or Saving a Configuration File

An import or export configuration can be saved and loaded, saving you the trouble of manually filling in the fields for multiple imports or exports. A configuration saved from an export can be loaded for an import, helping ensure that the file field positions, for example, correspond for both the import and export.

Delimiters

Delimiters are used in ASCII text files to separate items that represent fields and records in imported or exported data.

Default delimiters are associated with each delimiter type. A delimiter can be set to None, but if so, and the export encounters a condition requiring a delimiter, the export reports an error.

Between Fields: This delimiter is placed between each field.

Around Each Field: Use this delimiter to indicate the beginning and end of each field.

After Each Record: This delimiter is placed at the end of each record.

Between Values (Multi-Value Fields): Use this delimiter to separate the values in a multi-valued field. For example, an attribute such as "Group Membership" can have one or more values. Each Group Membership value is delimited by the multi-value field delimiter.

Between Elements (Multi-Element Values): Use this delimiter to separate the elements of a multi-element value. For example, an attribute having the syntax of SYN_OBJECT_ACL has three elements: the protected attribute name, the subject name, and the privileges.

Before Literal Characters: When you import an ASCII file created by a third-party export program, precede each literal character that is also a delimiter with the Before Literal Characters delimiter. If you use the Around Each Field delimiter, you do not need to precede literal characters within the field with the Before Literal Character delimiter.

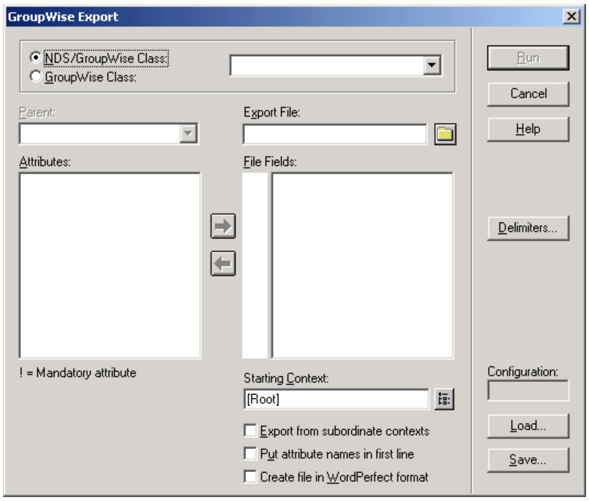
Export

The GroupWise Export utility reads eDirectory and GroupWise object information from GroupWise databases and creates an ASCII-delimited text file containing the object attributes. The Export utility supports most eDirectory classes (including extensions) and GroupWise classes. You can specify the delimiters, eDirectory contexts, and file field positions during export.

IMPORTANT: The Export utility is not included on the *GroupWise 6.5* CDs. You can download the Import/Export utility from TID 2960897 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp). To install the Import/Export utility, follow the instructions provided with the download. The Import/Export utility is not available for use on Linux.

To export objects from GroupWise:

1 In ConsoleOne, select the eDirectory tree that contains the GroupWise objects you want to export, click the Tools menu > GroupWise Utilities > Export to display the GroupWise Export dialog box.



● NDS/GroupWise Class:

○ GroupWise Class:

Starting Context: [Root]

□ Export from subordinate contexts

□ Put attribute names in first line

□ Create file in WordPerfect format

2 If you have previously defined and saved a configuration, click Load to fill in the fields from the configuration file, then click Run to perform the export.

or

Fill in the fields in the Export dialog box.

NDS/GroupWise Class: Select this option to export objects belonging to an eDirectory class or to a GroupWise-related eDirectory class. Choose the class from the list.

GroupWise Class: Select this option to export objects belonging to a GroupWise class not represented in eDirectory. Choose external user, external domain, external post office, Document-Version, or Lookup Entry from the list.

Parent: If you are exporting objects that belong to a GroupWise-related eDirectory class or a GroupWise-only class, and that class has a parent attribute, post office, or domain, this field allows you to export objects having only the parent attribute value you enter. The object selection process is still subject to the values in Starting Context, explained below, and the Export from Subordinate Contexts check box.

Export File: Specify the full path and file name of the ASCII text file.

Attributes / File Fields: This list displays the attributes of the selected class. Move the attributes to correspond to the fields in the ASCII text file to the File Fields list.

Some attributes are marked with an exclamation point (!), indicating that a value for that attribute must exist.

Starting Context: Specify the eDirectory context from which to begin the export. If the Export from Subordinate Contexts list box is checked, objects belonging to contexts subordinate to the context entered here is also exported.

Export from Subordinate Contexts: Check this box to cause objects in subordinate contexts to be exported. If this box is left unchecked, only those objects in the immediate Starting Context context are exported.

Put Attribute Names in First Line: Check this box to direct the export to put the attribute names as a comment in the first line of the export file.

Create the File in WordPerfect Office Notebook Format: If you use this option, you might also want to check Put Attribute Names in First Line to permit WordPerfect* to display the attribute names for each merge field.

Delimiters: Accept the defaults shown or change the delimiters. For more information, see "Delimiters" on page 70.

3 Click Run to perform the export.

New System

You can use the New System utility to create a new GroupWise system.

The process for creating a new GroupWise system is similar to the process of creating your initial GroupWise system (see "Installing a Basic GroupWise System" in the *GroupWise 6.5 Installation Guide*), except that you don't install the software from the *GroupWise 6.5* or *GroupWise 6.5 for Linux* CDs. Instead, during creation of the new system, you are asked to specify an existing software distribution directory to use in the new system. If you don't want to share software distribution directories between systems, you should create a new distribution directory. For information about creating software distribution directories, see "Software Directory Management" on page 57.

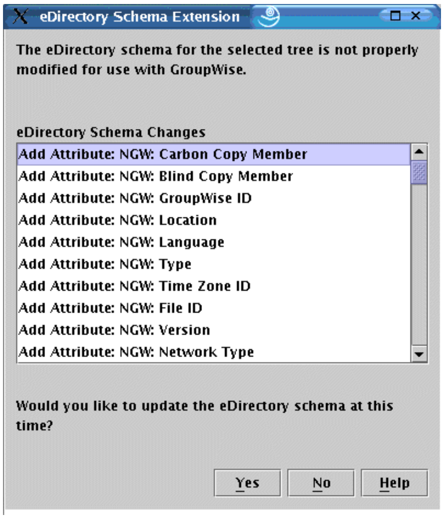
Check eDirectory Schema (Linux Only)

GroupWise systems include GroupWise-specific objects that are not available in eDirectory until the eDirectory schema for your eDirectory tree has been extended for these objects. Schema extension takes place automatically when you create a GroupWise system using the GroupWise Setup Advisor. In the Linux version of ConsoleOne, you can check an eDirectory tree to determine whether its schema has been extended for GroupWise.

In the Linux version of ConsoleOne:

1. Select a tree to check.
2. Click Tools > GroupWise Utilities > Check eDirectory Schema.

   If the eDirectory tree has not yet been extended for GroupWise, the eDirectory Schema Extension dialog box lists the changes that are required for GroupWise.



The eDirectory schema for the selected tree is not properly modified for use with GroupWise.

eDirectory Schema Changes

Add Attribute: NGW: Carbon Copy Member
Add Attribute: NGW: Blind Copy Member
Add Attribute: NGW: GroupWise ID
Add Attribute: NGW: Location
Add Attribute: NGW: Language
Add Attribute: NGW: Type
Add Attribute: NGW: Time Zone ID
Add Attribute: NGW: File ID
Add Attribute: NGW: Version
Add Attribute: NGW: Network Type

Would you like to update the eDirectory schema at this time?

3. Click Yes to extend the schema for GroupWise so that you can create GroupWise objects in the selected tree.

   or

   Click No if you decide you do not want to be able to create GroupWise objects in the selected tree.

If the schema of the tree has already been extended for GroupWise objects, a messages notifies you of this and you can immediately create new GroupWise objects in the selected tree.

GW / eDirectory Association

The GW / eDirectory Association menu includes the following options:

- "Graft GroupWise Objects" on page 74
- "Invalid Associations" on page 74
- "Associate Objects" on page 76
- "Disassociate GroupWise Attributes" on page 77
- "Convert External Entity to User" on page 77
- "Convert User to External Entity" on page 78

Graft GroupWise Objects

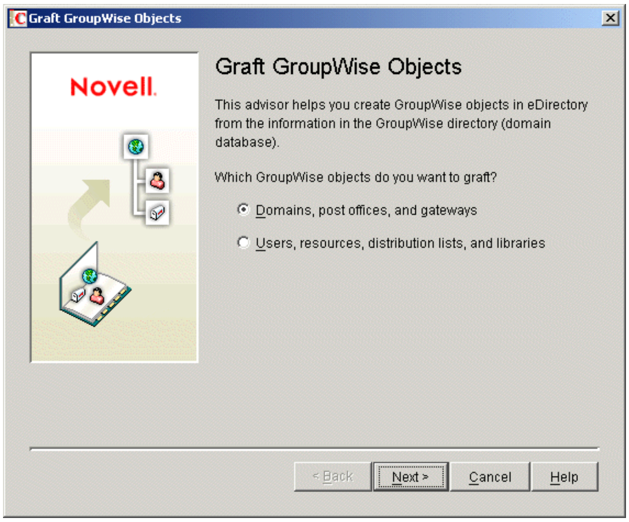
You can use the Graft GroupWise Objects utility to create GroupWise objects in the eDirectory tree from the information in your GroupWise domain database. The utility creates Domain, Post Office, and Gateway objects as well as User, Resource, and Distribution List objects. When grafting GroupWise user information from the GroupWise database into eDirectory, you can create a new User object and assign the GroupWise user information (account) to the User object, or you can match the GroupWise user information to an existing User object.

Grafting GroupWise objects from the GroupWise database into eDirectory can be useful in the following situations:

- The GroupWise database includes information that is not included in eDirectory.
- You want to move GroupWise information (domains, post offices, gateways, users, or resources) from one eDirectory tree to another.

To graft GroupWise objects:

1. In ConsoleOne, select a container in the eDirectory view.
2. Click the Tools menu > GroupWise Utilities > GW / eDirectory Associations > Graft GroupWise Object to display the Graft GroupWise Objects dialog box.



Graft GroupWise Objects

This advisor helps you create GroupWise objects in eDirectory from the information in the GroupWise directory (domain database).

Which GroupWise objects do you want to graft?

● Domains, post offices, and gateways

○ Users, resources, distribution lists, and libraries

3. Follow the on-screen prompts. If you need information about a dialog box, click the Help button.

Invalid Associations

Normally, a GroupWise object in eDirectory points to corresponding information in the GroupWise domain database. In turn, the information in the GroupWise domain database points back to its corresponding object in eDirectory.

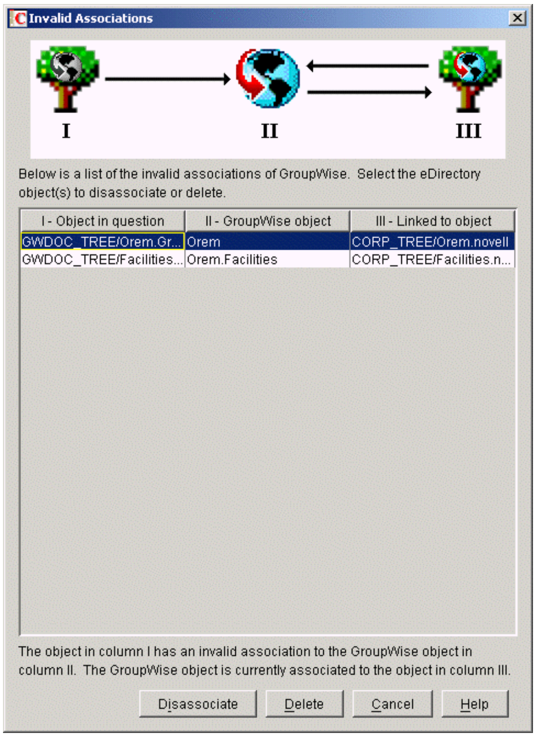
Occasionally, a situation might arise where information in the GroupWise domain database no longer points to the same eDirectory object that points to it. This results in an invalid association between the information in the two directories.

You can use the Invalid Associations utility to correct invalid associations between information in the GroupWise domain database and eDirectory.

To check for invalid associations:

1. In the eDirectory View in ConsoleOne, select the container whose objects you want to check for invalid associations (for example, an Organization, Organizational Unit, Domain, or Post Office).

2. Click the Tools menu > GroupWise Utilities > GW / eDirectory Associations > Invalid Associations to display the Invalid Associations dialog box.



Below is a list of the invalid associations of GroupWise. Select the eDirectory object(s) to disassociate or delete.

I - Object in question	II - GroupWise object	III - Linked to object
GWDOC_TREE/Orem.Gr...	Orem	CORP_TREE/Orem.novell
GWDOC_TREE/Facilities...	Orem.Facilities	CORP_TREE/Facilities.n...

The object in column I has an invalid association to the GroupWise object in column II. The GroupWise object is currently associated to the object in column III.

The dialog box lists each invalid association for the objects in the selected container. The dialog box fields are described below:

- **Object in Question (Column I):** This field lists the eDirectory object that has an invalid association to a GroupWise object. The eDirectory object points to the GroupWise object listed in column II, but the GroupWise object, according to the GroupWise domain database, does not point back to the eDirectory object.

- **GroupWise Object (Column II):** This field lists the GroupWise object to which the eDirectory object listed in column I is associated.

- **Linked to Object (Column III):** This field lists the eDirectory object to which the GroupWise object listed in column II has a valid association.

3. To remove the invalid association by disassociating the eDirectory object in Column I with the GroupWise object in Column II, select the association, then click Disassociate.

4. To remove the invalid association by deleting the eDirectory object listed in Column I, select the association, then click Delete.

Associate Objects

You can use the Associate Objects utility to associate GroupWise information with an eDirectory object.

For example, if you delete a user's eDirectory account but not his or her GroupWise account, the user's GroupWise information is retained as a GroupWise External User object in the GroupWise database and can be viewed in the GroupWise View. You can then associate the GroupWise External User object with another eDirectory User object. In essence, you are moving the GroupWise information from one eDirectory User object to another.

In some circumstances, it is possible for the link between an eDirectory User object and its GroupWise information to be lost. If this occurs, the GroupWise information, which still exists in the GroupWise database, appears as a GroupWise External User object in the GroupWise View. You can use the Associate Objects utility to reassociate the GroupWise information with the eDirectory User object.

The Associate Objects utility can be used to associate the following objects:

- GroupWise User or External User objects with eDirectory User objects
- GroupWise External Entity objects with eDirectory External Entity objects

Associating GroupWise User or External User Objects with eDirectory User Objects

To associate a GroupWise User or External User object with an eDirectory User object:

1 In the GroupWise View in ConsoleOne, select the GroupWise User or External User object you want.

   or

   In the eDirectory View, select the eDirectory User object you want.

2 Click the Tools menu > GroupWise Utilities > GW / eDirectory Associations > Associate Objects.

3 If you selected a GroupWise User or External User object in Step 1, select the eDirectory User object you want to associate with it.

   or

   If you selected an eDirectory User object in Step 1, select the GroupWise User object you want to associate with it.

4 Click OK to create the association.

   If the eDirectory User object is already associated with another GroupWise object, you receive a warning message indicating this. If you continue, the eDirectory User object is associated with the selected GroupWise object and its association with the other GroupWise object removed.

   If the GroupWise User or External User object is already associated with another eDirectory User object, you receive a warning message indicating this. If you continue, the GroupWise User object is associated with the selected eDirectory object and its association with the other eDirectory object removed.

Associating GroupWise External Entity Objects with eDirectory External Entity Objects

To associate a GroupWise External Entity object with an eDirectory External Entity object:

1. In the GroupWise View in ConsoleOne, select the GroupWise External Entity object you want.

   or

   In the eDirectory View, select the eDirectory External Entity object you want.

2. Click the Tools menu > GroupWise Utilities > GW / eDirectory Associations > Associate Objects.

3. If you selected a GroupWise External Entity object in Step 1, select the eDirectory External Entity object you want to associate with it.

   or

   If you selected an eDirectory External Entity object in Step 1, select the GroupWise External Entity object you want to associate with it.

4. Click OK to create the association.

   If the eDirectory External Entity object is already associated with another GroupWise object, you receive a warning message indicating this. If you continue, the eDirectory External Entity object is associated with the selected GroupWise object and its association with the other GroupWise object removed.

   If the GroupWise External Entity object is already associated with another eDirectory External Entity object, you receive a warning message indicating this. If you continue, the GroupWise External Entity object is associated with the selected eDirectory object and its association with the other eDirectory object removed.

Disassociate GroupWise Attributes

You can use the Disassociate GroupWise Attributes utility to disassociate GroupWise information from an eDirectory User object. This results in two separate eDirectory objects:

- The User object, which no longer includes any GroupWise information.
- A GroupWise External User object, which represents the user's record in the GroupWise database and is displayed only in the GroupWise View. The External User object allows the user to continue to have access to GroupWise and also enables you to graft the user record to another eDirectory User object. For more information, see "Graft GroupWise Objects" on page 74.

To disassociate the GroupWise attributes from an eDirectory User object:

1. In ConsoleOne, select the User object whose GroupWise attributes you want to remove.
2. Click the Tools menu > GroupWise Utilities > GW / eDirectory Associations > Disassociate GroupWise Attributes.

Convert External Entity to User

You can use the Convert External Entity to User utility to convert a GroupWise External Entity object to an eDirectory User object.

1. In ConsoleOne, select the GroupWise External Entity object that you want to convert to an eDirectory User object.

2. Click the Tools menu > GroupWise Utilities > GW / eDirectory Associations > Convert External Entity to User.
3. Click Yes to confirm that you want the conversion performed.

Convert User to External Entity

You can use the Convert User to External Entity utility to convert a User object to a GroupWise External Entity object.

1. In ConsoleOne, select the User object that you want to convert to an GroupWise External Entity object.
2. Click the Tools menu > GroupWise Utilities > GW / eDirectory Associations > Convert User to External Entity.
3. Click Yes to confirm that you want the conversion performed.

GroupWise Check Utility (GWCheck)

GroupWise Check is a standalone version of the ConsoleOne Mailbox/Library Maintenance utility. Like the Mailbox/Library Maintenance utility, GroupWise Check checks and repairs GroupWise user, message, library, and resource databases. However, in addition to checking post office, user, and library databases, it also checks users' remote, caching, and archive databases.

For information about using GroupWise Check, see "GroupWise Check" on page 391.

GroupWise Target Service Agent (GWTSA)

The GroupWise Target Service Agent (GWTSA) works with software backup programs to provide reliable backups of a running GroupWise system.

For information about using the GroupWise Target Service Agent, see "GroupWise Target Service Agent" on page 399.

GroupWise Backup Time Stamp Utility (GWTMSTMP)

The GroupWise Backup Time Stamp utility (GWTMSTMP) can be used to place a time stamp on a GroupWise user database to indicate the last time the database was backed up. If a user deletes an item from his or her mailbox and purges it from the Trash, the item is only deleted from the user's database if the time stamp shows that the item would have already been backed up. Otherwise, the item remains in the user's database until the database is backed up, at which time it is deleted from the working database.

For information about using the GroupWise Backup Time Stamp utility, see "GroupWise Time Stamp Utility" on page 405.

GroupWise Database Copy Utility (DBCOPY)

The GroupWise Database Copy utility (DBCOPY) copies files from a live GroupWise system to a static location for backup. During the copy process, DBCOPY prevents the files from being modified, using the same locking mechanism used by other GroupWise programs that access databases. This ensures that the backed-up versions are consistent with the originals even when large databases take a substantial amount of time to copy.

For information about using the GroupWise Database Copy utility, see “GroupWise Database Copy Utility” on page 412.

GroupWise Generate CSR Utility (GWCSRGEN)

To provide secure communication through an SSL (Secure Socket Layer) connection, the GroupWise Agents (MTA, POA, and Internet Agent) require access to a server certificate and private key.

You can use the GroupWise Generate CSR utility (GWCSRGEN) to generate a Certificate Signing Request (CSR) file and a Private Key file.

The CSR file, which is BASE64 encoded, contains the information required for a Certificate Authority (CA) to issue you a server certificate. This server certificate, when paired with the private key generated by the GroupWise Generate CSR utility, enables GroupWise agents to use SSL connections.

For information about SSL and certificates, see “Server Certificates and SSL Encryption” on page 1041.

6 GroupWise Addressing

Address Book

The GroupWise® Address Book contains information about all the addressable objects (users, resources, and distribution lists) that have been defined for your GroupWise system. Using the Address Book, GroupWise users can address items (messages, appointments, and so forth) or look up information about a user, resource, or distribution list.

You can determine how information is displayed in the Address Book, control the visibility of users, resources, and distribution lists in the Address Book, and update information when it gets out of sync. The following sections provide details:

NOTE: In addition to the administrator-controlled changes you can make to the Address Book, GroupWise users can make individual changes such as creating personal address books, sharing personal address books, and accessing LDAP address books. For information about the Address Book functionality available to users, see:

- "Using the Address Book" in the *GroupWise 6.5 Windows Client User Guide*
- "Using the Address Book" in the *GroupWise 6.5 WebAccess Client User Guide*
- "Using the Address Book" in the *GroupWise 6.5 Cross-Platform Client User Guide*

Determining Fields, Field Order, and Sort Order for the Address Book

The GroupWise Address Book is configured to display specific user fields such as Given Name and Last Name, but you can add additional fields or delete the default fields. You can also determine the order in which the fields appear in the Address Book and select whether the addresses is sorted by first name/last name or last name/first name.

The GroupWise Address Book is configured at the domain level, which means that you can have different fields, field order, or sorting order for the Address Book in different domains.

The Address Book configuration you establish for a domain becomes the default configuration. However, users can change which fields are displayed, change the field order, and change the address sort order. However, they cannot add fields that you have not added at the domain level.

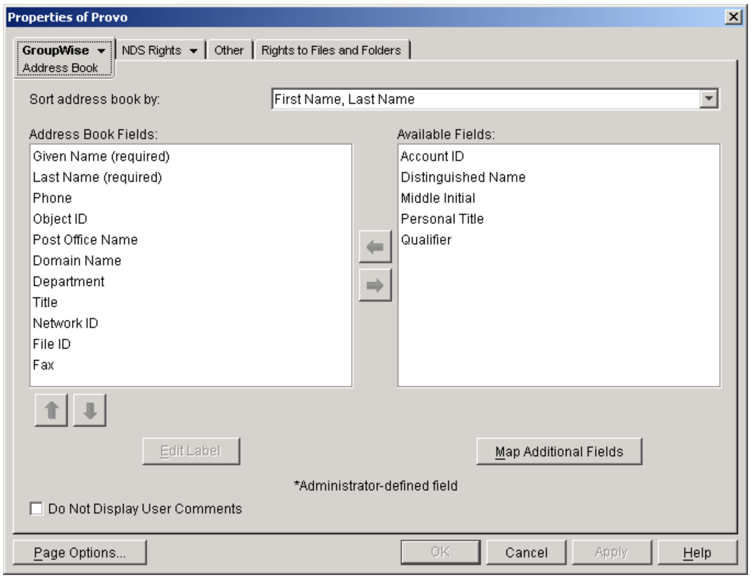
The following sections provide instructions for adding and deleting Address Book fields, changing the default sort order of the Address Book, and changing the default order of the fields in the Address Book:

- "Adding Fields to the Address Book" on page 82
- "Changing the Default Sort Order" on page 83
- "Changing the Default Field Order" on page 83
- "Removing Fields from the Address Book" on page 84
- "Preventing the User Description Field from Displaying in the Address Book" on page 85

Adding Fields to the Address Book

Adding a field makes the field available in the Address Book. However, individual users can determine which available fields they want to display.

1. In ConsoleOne®, right-click the Domain object whose Address Book you want to modify, then click Properties.
2. Click GroupWise > Address Book to display the Address Book page.



Properties of Provo

Sort address book by: First Name, Last Name

Address Book Fields:
Given Name (required)
Last Name (required)
Phone
Object ID
Post Office Name
Domain Name
Department
Title
Network ID
File ID
Fax

Available Fields:
Account ID
Distinguished Name
Middle Initial
Personal Title
Qualifier

*Administrator-defined field

☐ Do Not Display User Comments

The Address Book Fields list shows all fields that are displayed by default in the Address Book.

The Available Fields list shows additional predefined GroupWise user fields that can be added to the Address Book. Novell® eDirectory™ also includes user information that is not associated to GroupWise user fields. For example, a User object includes Postal Address fields named "City," "State," and "Zip Code." By default, these fields are not included as GroupWise fields. However, you can use the Map Additional Fields button to map eDirectory user fields to GroupWise fields so that they can be displayed in the GroupWise Address Book.

3. To add a field that is not displayed in the Available Fields list, click Map Additional Fields, select an unmapped Admin-defined field, click Edit, select the eDirectory property to map to the Admin-defined field, then click OK twice to add it to the Available Fields list.
4. In the Available Fields list, select the field you want to add to the Address Book, then click the left-arrow to move it to the Address Book Fields list.

The field is added to the bottom of the list. The Address Book displays the fields in the order they are listed.

5 If necessary, select the field, then use the up-arrow and down-arrow to move the field to the appropriate location in the list.

6 If the field is an Administrator-defined field and you want to change how the field is labeled in the Address Book, select the field, click Edit Label, enter a new label in the Address Book Label field, then click OK.

   Administrator-defined fields are marked with an asterisk (*). You can only edit an Administrator-defined field that is in the Address Book Fields list.

7 When you are finished, click OK (in the Address Book page) to save your changes.

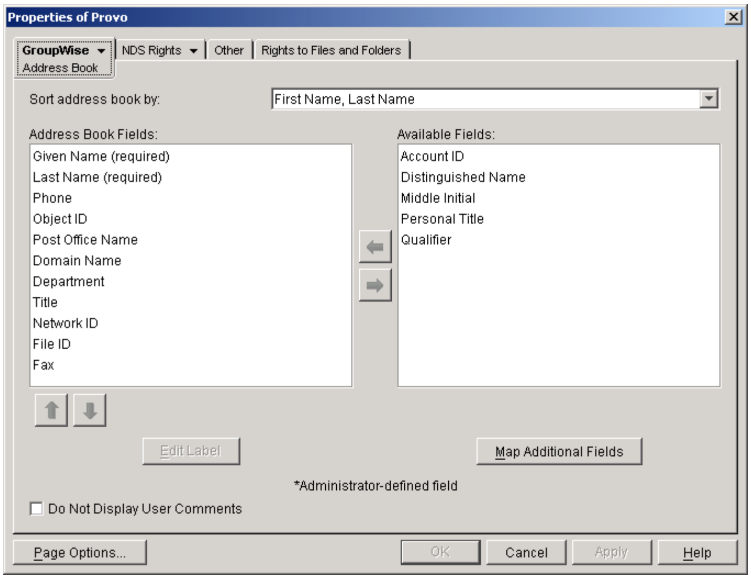
Changing the Default Sort Order

The sort order determines how addresses in the Address Book are sorted. The sort order you establish becomes the default for the Address Book and remains in effect until individual users change it.

The preset default sort order for the Address Book is First Name/Last Name. You can change the default sort order to Last Name/First Name.

1 In ConsoleOne, right-click the Domain object whose Address Book you want to modify, then click Properties.

2 Click GroupWise > Address Book to display the Address Book page.



Properties of Provo

Sort address book by: First Name, Last Name

Address Book Fields:
Given Name (required)
Last Name (required)
Phone
Object ID
Post Office Name
Domain Name
Department
Title
Network ID
File ID
Fax

Available Fields:
Account ID
Distinguished Name
Middle Initial
Personal Title
Qualifier

*Administrator-defined field

□ Do Not Display User Comments

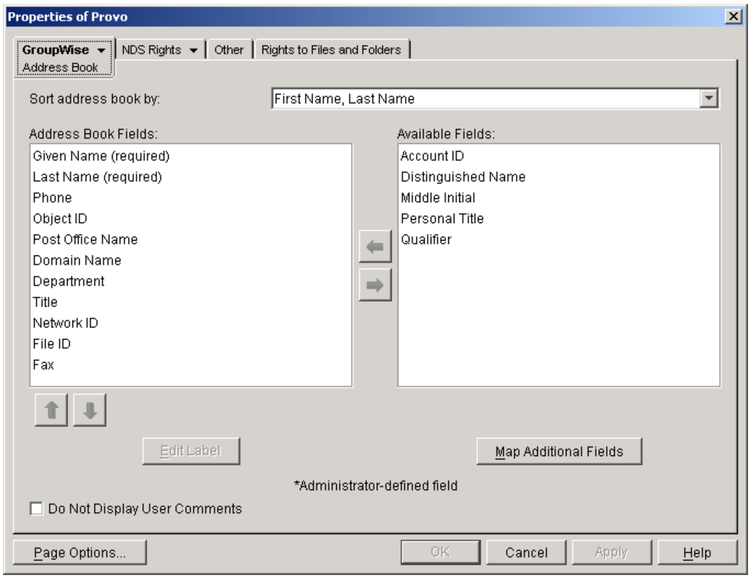
3 In the Sort Address Book By list, select the sort order you want to be the default.

4 Click OK to save your changes.

Changing the Default Field Order

The field order determines the order in which the GroupWise fields are displayed in the Address Book. The field order you establish becomes the default for the Address Book and remains in effect until individual users change the order.

1. In ConsoleOne, right-click the Domain object whose Address Book you want to modify, then click Properties.
2. Click GroupWise > Address Book to display the Address Book page.



Sort address book by: First Name, Last Name

Address Book Fields:
Given Name (required)
Last Name (required)
Phone
Object ID
Post Office Name
Domain Name
Department
Title
Network ID
File ID
Fax

Available Fields:
Account ID
Distinguished Name
Middle Initial
Personal Title
Qualifier

*Administrator-defined field

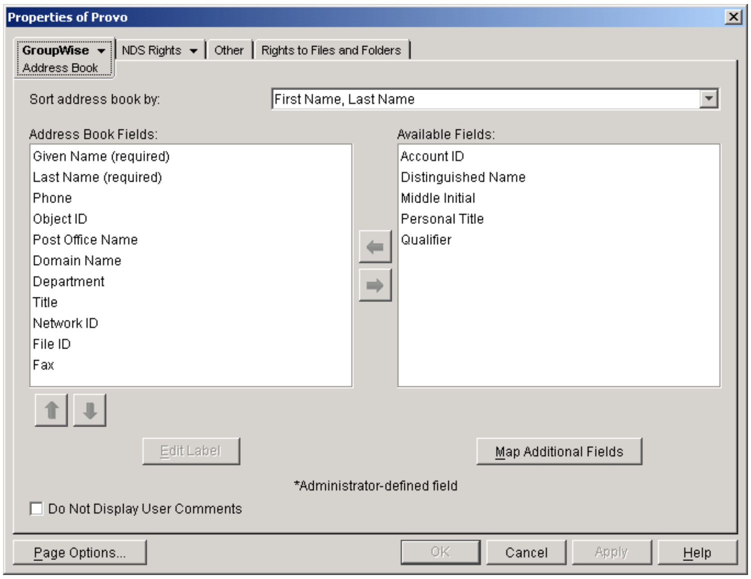
□ Do Not Display User Comments

3. In the Address Book Fields list, select a field whose position you want to change, then use the up-arrow and down-arrow to move the field to its new position.
4. Repeat Step 3 until you've established the field order you want.
5. Click OK to save your changes.

Removing Fields from the Address Book

If there are fields in the Address Book that are not used or that you don't want displayed to users, you can remove them.

1. In ConsoleOne, right-click the Domain object whose Address Book you want to modify, then click Properties.
2. Click GroupWise > Address Book to display the Address Book page.



Sort address book by: First Name, Last Name

Address Book Fields:

Given Name (required)
Last Name (required)
Phone
Object ID
Post Office Name
Domain Name
Department
Title
Network ID
File ID
Fax

Available Fields:

Account ID
Distinguished Name
Middle Initial
Personal Title
Qualifier

*Administrator-defined field

☐ Do Not Display User Comments

3 In the Address Book Fields list, select the field you want to remove, then click the right-arrow to move the field to the Available Fields list.

The fields in the Available Fields list are not displayed in the Address Book.

4 Repeat Step 3 to remove additional fields you don’t want to use.

5 Click OK to save your changes.

Preventing the User Description Field from Displaying in the Address Book

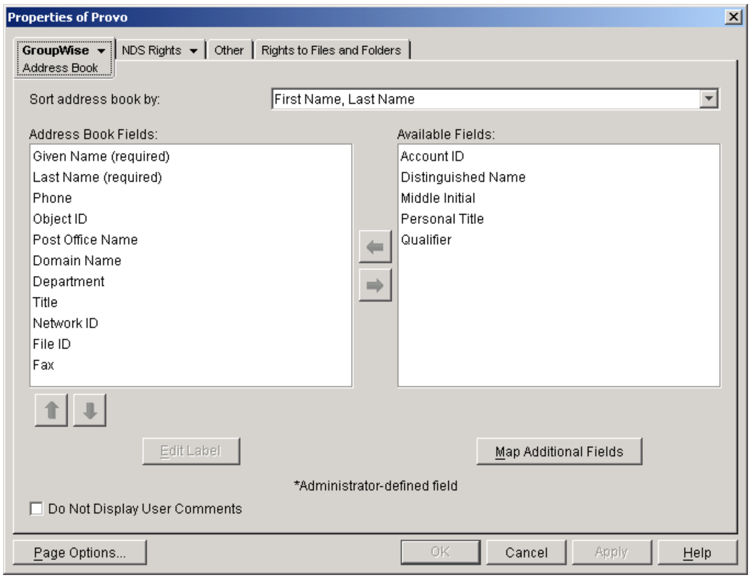
The GroupWise Address Book provides detailed user information as well as e-mail addresses. A user’s detailed information includes a comments field that displays the information stored in the User object Description field (User object > General tab > Identification page). If you have included information in the Description field that you don’t want displayed in the GroupWise Address Book, you can prevent the field’s contents from being displayed.

TIP: To view a user’s detailed information, including the comments field, in the Address Book, select the user’s address, then click the View menu > Details.

To prevent the user description from appearing the Address Book:

1 In ConsoleOne, right-click the Domain object whose Address Book you want to modify, then click Properties.

2 Click GroupWise > Address Book to display the Address Book page.



Sort address book by: First Name, Last Name

Address Book Fields:

- Given Name (required)
- Last Name (required)
- Phone
- Object ID
- Post Office Name
- Domain Name
- Department
- Title
- Network ID
- File ID
- Fax

Available Fields:

- Account ID
- Distinguished Name
- Middle Initial
- Personal Title
- Qualifier

*Administrator-defined field

□ Do Not Display User Comments

3 Enable the Do Not Display User Comments option.

4 Click OK to save your changes.

Controlling Object Visibility in the Address Book

An object's visibility determines which post office databases the object's information is distributed to. A post office's users can only see an object's information in the Address Book if the object's information has been distributed to its post office.

Visibility applies to the following objects: user, external user, external entity, resource, external resource, distribution list, eDirectory group, eDirectory organizational role, and nickname.

IMPORTANT: Unlike the other objects listed above, nicknames that have been distributed to a post office do not actually appear in the post office's Address Book. Users must type the nickname's address in the message rather than select it from the Address Book.

You can choose from the following visibility levels:

- **System:** The object is visible in every post office Address Book throughout the system; if external system synchronization is turned on, it is also available for distribution to other GroupWise systems. This is the default for users, external users, resources, external resources, external entities, and nicknames.
- **Domain:** The object is visible only in the Address Book of the post offices located in the object's domain.
- **Post Office:** The object is visible only in the Address Book of the object's post office. This is the default for distribution lists, groups, and organizational roles.
- **None:** The object is not visible in the Address Book of any post offices.

For information about setting visibility, see:

- "Changing a User's Visibility in the Address Book" on page 212
- "Changing a Resource's Visibility in the Address Book" on page 232
- "Changing a Distribution List's Visibility in the Address Book" on page 246
- "Changing a Group's Visibility in the Address Book" on page 253
- "Changing an Organizational Role's Visibility in the Address Book" on page 257

Updating Address Book Information

Each post office database includes all the information displayed in the GroupWise Address Book. By keeping the information on the post office, the post office's users have quick access to it. Whenever changes are made in eDirectory that affect Address Book information, the information is replicated to each domain database and each post office database.

If information in a post office's Address Book is out-of-date or missing, you can synchronize the missing information with eDirectory or rebuild the post office database to update the information.

The following sections provide details:

- "Synchronizing Information" on page 87
- "Rebuilding the Post Office Database" on page 87

Synchronizing Information

The information for each object (user, resource, distribution list, and so forth) in the GroupWise Address Book is contained in eDirectory. When an object's information is incorrect in a post office's Address Book, you can synchronize the object's information in the Address Book with the information stored in eDirectory. This causes the correct information to be replicated to each domain and post office database in the GroupWise system. For information about how to do this, see Chapter 29, "Synchronizing Database Information," on page 363.

Rebuilding the Post Office Database

If the post office Address Book is missing a lot of information, or you are having other difficulties with information in the Address Book, you might want to rebuild the post office's database. This causes all information to be replicated to the post office database from the domain database. For information about rebuilding a post office database, see "Rebuilding Domain or Post Office Databases" on page 349.

Internet-Style Addressing

By default, GroupWise® uses a proprietary address format consisting of a user's ID, post office, and domain (*userID.post_office.domain*). However, if you have the GroupWise Internet Agent installed (see "Internet Agent" on page 659), GroupWise also supports native Internet-style addressing consisting of a username and Internet domain name (for example, *userID@Internet_domain_name*).

Internet-style addressing is the preferred addressing format if you are connected to the Internet, because with Internet-style addressing, users have the same address within the GroupWise system as they do outside the GroupWise system. For example, if John Smith's address at Novell® is jsmith@novell.com, this address can be used by users within the GroupWise system and users external to the system.

The following sections provide information to help you plan, set up, and troubleshoot any problems that might occur:

- "Planning Internet Addressing" on page 88
- "Setting Up Internet Addressing" on page 91

Planning Internet Addressing

The following sections help you prepare to set up Internet-style addressing on your GroupWise system:

- "Internet Agent Requirement" on page 88
- "Internet Agents Used for Outbound Messages" on page 88
- "Internet Domain Names" on page 88
- "Preferred Address Format" on page 89
- "Allowed Address Formats" on page 91
- "Override Options" on page 91

Internet Agent Requirement

Internet addressing requires you to have the GroupWise Internet Agent installed in your GroupWise system. The Internet Agent connects your GroupWise system to the Internet. To install the Internet Agent, see "Installing the GroupWise Internet Agent" in the *GroupWise 6.5 Installation Guide*.

Internet Agents Used for Outbound Messages

Each domain in your GroupWise system must be assigned an Internet Agent for outbound messages. A domain's assigned Internet Agent handle all outbound messages sent by the domain's users.

If your GroupWise system includes only one Internet Agent, that Internet Agent must be assigned to all domains and will be used for all outbound messages.

If your GroupWise system includes multiple Internet Agents, you must decide which Internet Agent you want to be responsible for outbound messages for each domain. You must select one Internet Agent as your system's default Internet Agent, but you can override the default at each domain.

Internet Domain Names

You must associate at least one Internet domain (novell.com, gw.novell.com, support.novell.com, or so forth) with your GroupWise system. These Internet domains need to exist in the domain name service (DNS).

After you have associated Internet domains with your GroupWise system, all users in your system can be addressed using any of the domains (for example, jsmith@novell.com, jsmith@gw.novell.com, and jsmith@support.novell.com). The addresses can be used both internally and externally.

Preferred Internet Domain Name

You must assign each GroupWise user a preferred Internet domain. GroupWise uses the preferred Internet domain name when constructing the e-mail address that are displayed in the GroupWise Address Book and in the To field of sent messages.

To make this process easier, GroupWise lets you assign a preferred Internet domain to be used as the default for your GroupWise system (for example, novell.com). The system's preferred Internet domain is applied to all users in your GroupWise system. However, you can override the system's preferred Internet domain at the domain, post office, or user level, meaning that different users within your GroupWise system can be assigned different preferred Internet domains. For example, users in one domain can be assigned gw.novell.com as their preferred Internet domain while users in another domain are assigned support.novell.com.

Preferred Address Format

You must choose a preferred address format for your GroupWise users. GroupWise uses the preferred address format, along with the preferred Internet domain, to construct the e-mail addresses that are published in the GroupWise Address Book and in the To field of sent messages.

GroupWise supports the following address formats:

userID.post_office.domain@internet_domain_name
userID.post_office@internet_domain_name
userID@internet_domain_name
firstname.lastname@internet_domain_name
lastname.firstname@internet_domain_name
firstinital lastname@internet_domain_name

As with the preferred Internet domain, you must assign a preferred address format to be used as the default for your GroupWise system. The system's preferred address format is applied to all users in your GroupWise system. However, you can override the system's preferred address format at the domain, post office, and user/resource level.

The following sections explain some of the advantages and disadvantages of each address format:

- "userID.post_office.domain@internet_domain_name" on page 89
- "userID.post_office@internet_domain_name" on page 89
- "userID@internet_domain_name" on page 90
- "firstname.lastname@internet_domain_name" on page 90
- "lastname.firstname@internet_domain_name" on page 90
- "firstinitial lastname@internet_domain_name" on page 90

userID.post_office.domain@internet_domain_name

Advantages

- Reliable format. GroupWise guarantees that each address is unique.
- Identical usernames can be used in different post offices.

Disadvantages

- Addresses tend to be long and hard to remember.
- Addresses might change over time as users are moved from one post office to another.

userID.post_office@internet_domain_name

Advantages

- Guarantees uniqueness if all your post offices have unique names.
- Identical usernames can be placed in different post offices.

Disadvantages

- Addresses tend to be long and hard to remember.
- Addresses might change over time as users are moved from one post office to another.

userID@internet_domain_name

Advantages

- Addresses are short and easy to remember.
- Backwards-compatible with previous versions of GroupWise. (Users won't need to update their business cards.)
- Addresses do not change as users are moved.

Disadvantages

- Because GroupWise cannot guarantee unique user IDs, the system administrator is responsible for guaranteeing that the first and last names are unique.

firstname.lastname@internet_domain_name

Advantages

- Addresses are intuitive and easy to remember.
- Addresses do not change as users are moved.

Disadvantages

- Because GroupWise cannot guarantee unique first and last names, the system administrator is responsible for guaranteeing that the first and last names are unique.
- Probability of conflicts increases if any user's first and last names match any GroupWise domain or post office name, if any two users have the same first and last names, or if any two users have the opposite first and last names (such as James Dean and Dean James).

lastname.firstname@internet_domain_name

Advantages

- Addresses are intuitive and easy to remember.
- Addresses do not change as users are moved.

Disadvantages

- Because GroupWise cannot guarantee unique first and last names, the system administrator is responsible for guaranteeing that the first and last names are unique.
- Probability of conflicts increases if any user's first and last names match any GroupWise domain or post office name, if any two users have the same first and last names, or if any two users have the opposite first and last names (such as James Dean and Dean James).

firstinitial lastname@internet_domain_name

Advantages

- Addresses are intuitive and easy to remember.
- Addresses do not change as users are moved.

Disadvantages

- Because GroupWise cannot guarantee unique first initials and last names, the system administrator is responsible for guaranteeing that firstinitial lastname addresses are unique.

Allowed Address Formats

The preferred Internet domain and preferred address format apply to user addresses as displayed in the GroupWise Address Book or sent messages.

The allowed address formats, on the other hand, determine which address formats are accepted by the Internet Agent. There are five possible allowed formats:

userID.post_office@internet_domain_name
userID@internet_domain_name
firstname.lastname@internet_domain_name
lastname.firstname@internet_domain_name
firstinital lastname@internet_domain_name

If you select all five formats, the Internet Agent accepts messages addressed to users in any of the formats. For example, John Peterson would receive messages sent using any of the following addresses:

jpeterson.research@novell.com
jpeterson@novell.com
john.peterson@novell.com
peterson.john@novell.com
jpeterson@novell.com

You must designate the allowed address formats to be used as the default formats for your GroupWise system. The system's allowed address formats are applied to all users in your GroupWise system. However, you can override the system's allowed address formats at the domain, post office, and user/resource level.

For example, assume you have two John Petersons with userIDs of jpeterson and japeterson. The *userID.post_office* and *userID* address formats do not cause message delivery problems, but the *firstname.lastname*, *lastname.firstname*, and *firstinitial lastname* address formats do. To overcome this problem, you could disallow the three problem formats for these users at the user level.

Override Options

In spite of the best planning, some e-mail addresses do not fit the rules and are not processed correctly. You can handle such addresses by overriding the regular address processing, as described in "Overriding Internet Addressing Defaults" on page 94.

Setting Up Internet Addressing

The following sections help you to set up Internet addressing:

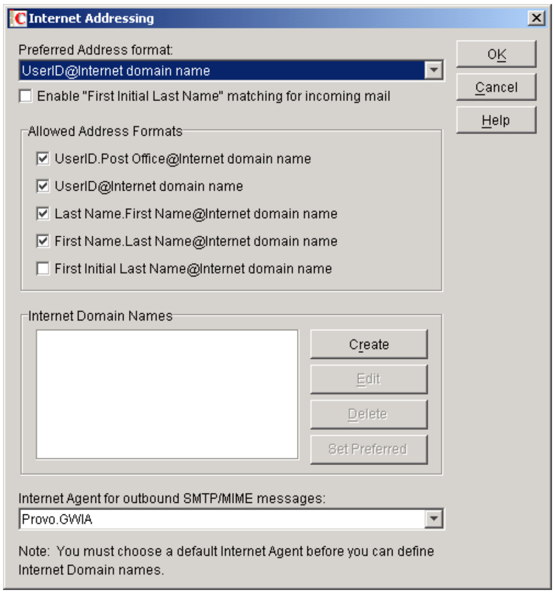
- "Installing the Internet Agent" on page 92
- "Enabling Internet Addressing" on page 92
- "Overriding Internet Addressing Defaults" on page 94

Installing the Internet Agent

Before you can set up Internet addressing, you must install the GroupWise Internet Agent. If you have not already installed the agent, see "Installing the GroupWise Internet Agent" in the *GroupWise 6.5 Installation Guide*.

Enabling Internet Addressing

1 In ConsoleOne, click the Tools menu > GroupWise System Operations > Internet Addressing.



Preferred Address format: UserID@Internet domain name

□ Enable "First Initial Last Name" matching for incoming mail

Allowed Address Formats

☑ UserID.Post Office@Internet domain name

☑ UserID@Internet domain name

☑ Last Name.First Name@Internet domain name

☑ First Name.Last Name@Internet domain name

□ First Initial Last Name@Internet domain name

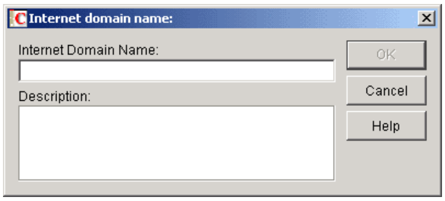
Internet Agent for outbound SMTP/MIME messages: Provo.GWIA

Note: You must choose a default Internet Agent before you can define Internet Domain names.

2 In the Internet Agent for Outbound SMTP/MIME Messages list, select the Internet Agent to use as the default Internet Agent for your system.

By default, each domain uses this Internet Agent for outbound messages sent by users in the domain. If you have multiple Internet Agents in your GroupWise system, you can override the default setting at the domain level. For more information, see "Domain Overrides" on page 94.

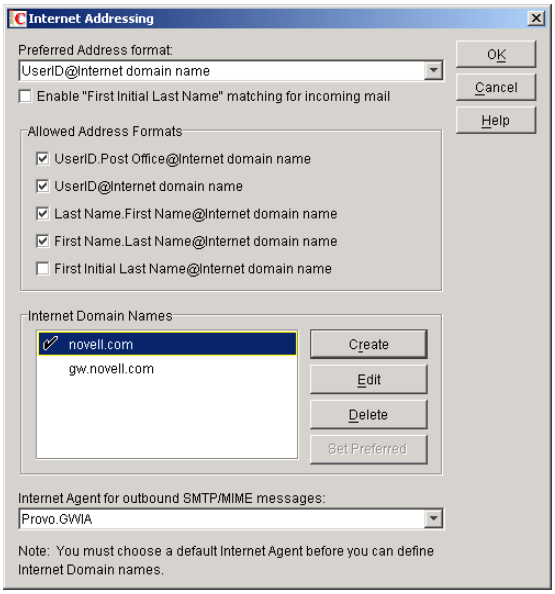
3 To define an Internet domain, click Create to display the Internet Domain Name dialog box.



4 Enter the Internet domain you want to define in your GroupWise system, then click OK to add it to the list of Internet domains.

5 Repeat Step 3 and Step 4 for each Internet domain you want to define.

When you've finished, all Internet domains you want to define should be listed in the Internet Domain Names box.



Preferred Address format: UserID@Internet domain name

□ Enable "First Initial Last Name" matching for incoming mail

Allowed Address Formats

☑ UserID.Post Office@Internet domain name
☑ UserID@Internet domain name
☑ Last Name.First Name@Internet domain name
☑ First Name.Last Name@Internet domain name
□ First Initial Last Name@Internet domain name

Internet Domain Names

✓ novell.com
gw.novell.com

Internet Agent for outbound SMTP/MIME messages: Provo.GWIA

Note: You must choose a default Internet Agent before you can define Internet Domain names.

The preferred Internet domain is indicated by a check mark. This is the Internet domain name that is used when GroupWise constructs a user's preferred e-mail address. A preferred e-mail address is the address that is published in the system address book and in the To field of sent messages. You can override the preferred Internet domain name at the domain, post office, and user/resource levels. For more information, see "Overriding Internet Addressing Defaults" on page 94.

6 If the Internet domain you want to be the default preferred domain for your GroupWise system is not already selected, select the desired Internet domain, then click Set Preferred Name.

7 In the Preferred Address Format list, select your system's default Internet address format.

This is the format that is used when displaying addresses in the GroupWise Address Book and in a message's From box if it is not overridden at a lower level. For a list of the available addressing formats and their respective advantages and disadvantages, see "Preferred Address Format" on page 89.

You can override the preferred address format at the domain, post office, and user/resource levels. For more information, see "Overriding Internet Addressing Defaults" on page 94.

8 If desired, turn on the Enable "First Initial Last Name" Matching for Incoming Mail option.

This option allows the Internet Agent to resolve addresses for incoming messages by performing "first initial last name" lookups on the username portion of the address. When doing so, the Internet Agent uses the first letter of the username as the first initial and the remainder of the username as the last name. It then resolves the address to any GroupWise users whose Last Name field (in their eDirectory User object record) contains the last name and whose Given Name field starts with the first initial.

For example, if the recipient's address is jpeterson@novell.com, the first initial would be J and the last name would be Peterson. The address would resolve to the user whose Last Name field is Peterson and Given Name field starts with J. If more than one user's given name starts with J (for example, John and Janice), the message is undeliverable.

This option is useful if you want to be able to use the UserID@Internet_domain_name format but your userIDs do not really reflect your users' actual names (for example, John Peterson's user ID is 46789 so his address is 46789@novell.com). In this case, you could publish users' addresses as their first initial last name (for example, jpeterson@novell.com) and enable this option so that the Internet Agent resolves the addresses to the appropriate users.

9 In the Allowed Address Formats list, select the address formats that you want to be supported for incoming messages. GroupWise will deliver a message to the recipient if any of the allowed formats have been used in the address.

You can override the allowed address formats at the domain, post office, and user/resource levels. For more information, see "Overriding Internet Addressing Defaults" on page 94.

10 Click OK to save your changes.

If you changed the preferred address format, you are prompted to update the Internet e-mail address (General tab > Identification page > E-Mail Address field) for all affected users. The Internet e-mail address is the address returned in response to LDAP queries to eDirectory. It is recommended that you allow this update; however, performing it for the entire GroupWise system might take a while.

At this point, Internet addressing is enabled.

Overriding Internet Addressing Defaults

All domains, post offices, and users/resources in your GroupWise system inherit the defaults (Internet Agent for outbound messages, preferred Internet domain name, preferred address format, and allowed address formats) you established when enabling Internet addressing for your system. However, if desired, you can override these defaults for individual domains, post offices, or users/resources.

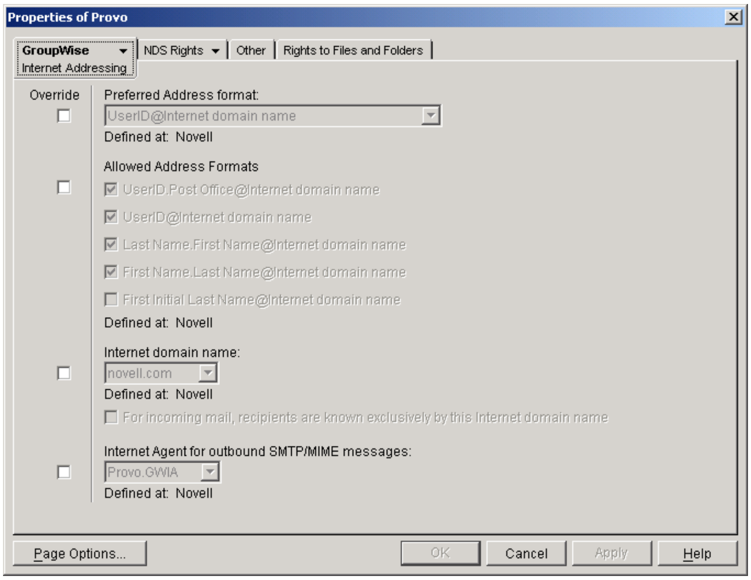
- "Domain Overrides" on page 94
- "Post Office Overrides" on page 95
- "User/Resource Overrides" on page 96

Domain Overrides

At the domain level, you can override all Internet addressing defaults assigned to your GroupWise system.

1 In ConsoleOne, right-click a Domain object, then click Properties.

2 Click GroupWise > Internet Addressing.



□ Preferred Address format: UserID@Internet domain name
Defined at: Novell

□ Allowed Address Formats
☑ UserID.Post Office@Internet domain name
☑ UserID@Internet domain name
☑ Last Name.First Name@Internet domain name
☑ First Name.Last Name@Internet domain name
□ First Initial Last Name@Internet domain name
Defined at: Novell

□ Internet domain name: novell.com
Defined at: Novell
□ For incoming mail, recipients are known exclusively by this Internet domain name

□ Internet Agent for outbound SMTP/MIME messages: Provo.GWIA
Defined at: Novell

3 To override one of the options, select the Override box, then select the option you prefer for this domain.

If you need additional information about any of the fields, click Help.

4 Click OK to save the changes.

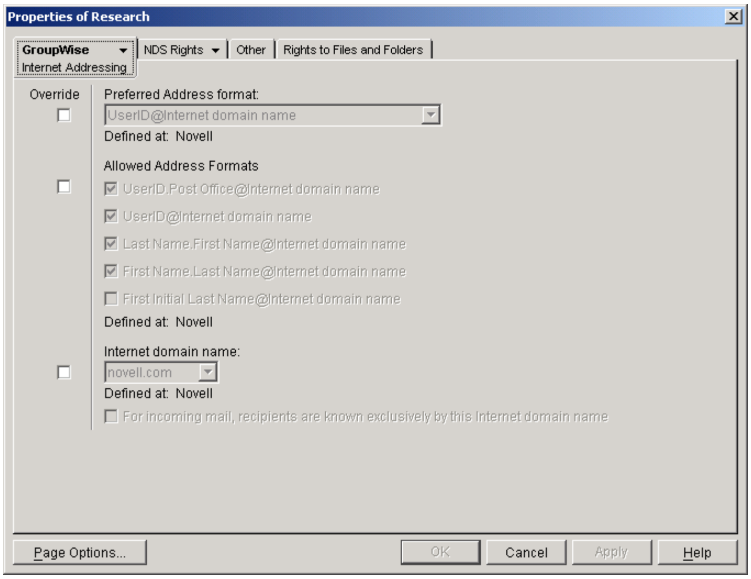
If you changed the preferred address format, you are prompted to update the Internet e-mail address (General tab > Identification page > E-Mail Address field) for all affected users. The Internet e-mail address is the address returned in response to LDAP queries to eDirectory. We recommend that you allow this update; however, performing it for an entire GroupWise domain might take a while.

Post Office Overrides

At the post office level, you can override the preferred Internet domain name, preferred address format, and allowed address formats the post office has inherited from its domain. You cannot override the Internet Agent that is assigned to handle outbound messages.

1 In ConsoleOne, right-click a Post Office object, then click Properties.

2 Click GroupWise > Internet Addressing.



Override

□ Preferred Address format: UserID@Internet domain name

Defined at: Novell

□ Allowed Address Formats

☑ UserID.Post Office@Internet domain name

☑ UserID@Internet domain name

☑ Last Name.First Name@Internet domain name

☑ First Name.Last Name@Internet domain name

□ First Initial Last Name@Internet domain name

Defined at: Novell

□ Internet domain name: novell.com

Defined at: Novell

□ For incoming mail, recipients are known exclusively by this Internet domain name

3 To override one of the options, select the Override box, then select the option you prefer for this post office.

If you need additional information about any of the fields, click Help.

4 Click OK to save the changes.

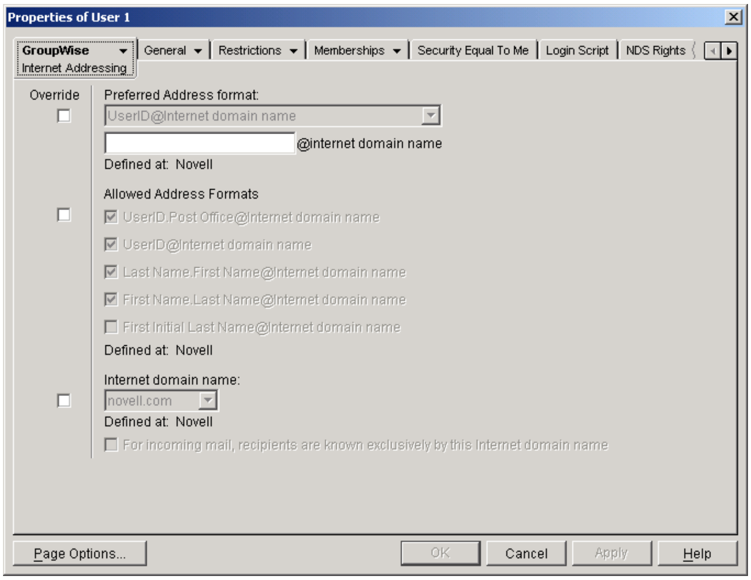
If you changed the preferred address format, you are prompted to update the Internet e-mail address (General tab > Identification page > E-Mail Address field) for all affected users. The Internet e-mail address is the address returned in response to LDAP queries to eDirectory. We recommend that you allow this update; however, performing it for an entire GroupWise post office might take a while.

User/Resource Overrides

At the user and resource level, you can override the preferred Internet domain, preferred address format, and allowed address formats that the user/resource has inherited from its post office. You cannot override the Internet Agent that is assigned to handle outbound messages.

1 In ConsoleOne, right-click a User or Resource object, then click Properties.

2 Click GroupWise > Internet Addressing.



Override

□ Preferred Address format: UserID@Internet domain name

@internet domain name

Defined at: Novell

□ Allowed Address Formats

☑ UserID.Post Office@Internet domain name

☑ UserID@Internet domain name

☑ Last Name.First Name@Internet domain name

☑ First Name.Last Name@Internet domain name

□ First Initial Last Name@Internet domain name

Defined at: Novell

□ Internet domain name: novell.com

Defined at: Novell

□ For incoming mail, recipients are known exclusively by this Internet domain name

3 To override one of the options, select the Override box, then select the option you prefer for this user or resource.

At the user and resource level, the preferred address format can be completely overridden by explicitly defining the user portion of the address format (*user@Internet domain name*). The user portion can include any RFC-compliant characters (no spaces, commas, and so forth).

For example, if you've selected *First Name.Last Name@Internet domain name* as your system's preferred address format and you have two John Petersons, each on a different post office in your system, you would end up two users having the same address (John.Peterson@novell.com). You could use this field to differentiate them by including their middle initials in their address (John.S.Peterson@novell.com and John.A.Peterson@novell.com).

If you need additional information about any of the fields, click Help.

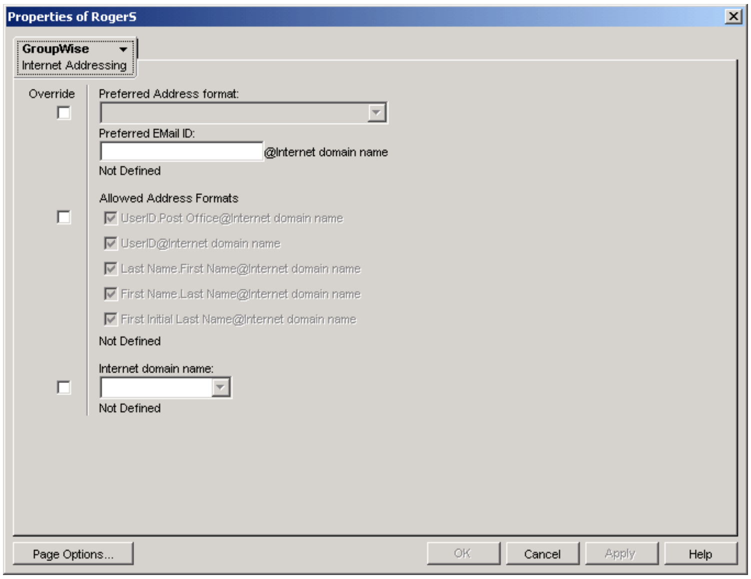
4 Click OK to save the changes.

If you changed the preferred address format for a user, you are prompted to update the user's Internet e-mail address (General tab > Identification page > E-Mail Address field). The Internet e-mail address is the address returned in response to LDAP queries to eDirectory. We recommend that you allow this update.

Nickname Overrides

At the nickname level, you can override the preferred Internet domain, preferred address format, and allowed address formats that the user/resource has inherited from its post office. You cannot override the Internet Agent that is assigned to handle outbound messages.

1. In the GroupWise View of ConsoleOne, select Nicknames in the GroupWise Object list.
2. Right-click a nickname, then click Properties.
3. Click GroupWise > Internet Addressing.



Override

□ Preferred Address format:

Preferred EMail ID: @Internet domain name

Not Defined

□ Allowed Address Formats

☑ UserID.Post Office@Internet domain name

☑ UserID@Internet domain name

☑ Last Name.First Name@Internet domain name

☑ First Name.Last Name@Internet domain name

☑ First Initial Last Name@Internet domain name

Not Defined

□ Internet domain name:

Not Defined

4. To override one of the options, select the Override box, then select the option you prefer for this nickname.
5. Click OK to save the changes.

   If you changed the preferred address format for a nickname, you are prompted to update the user's Internet e-mail address (General tab > Identification page > E-Mail Address field). The Internet e-mail address is the address returned in response to LDAP queries to eDirectory. We recommend that you allow this update.

For more information about nicknames, see "Creating a Nickname for a User" on page 213.

Addressing Rules

Addressing rules let you search for text in an address and replace it with other text. Most addressing rules are used in conjunction with GroupWise® gateways to simplify addressing syntax. For specific details, see your GroupWise gateway guide. For an example of an addressing rule used with the Internet Agent, see "Creating a Customized Addressing Rule" on page 700.

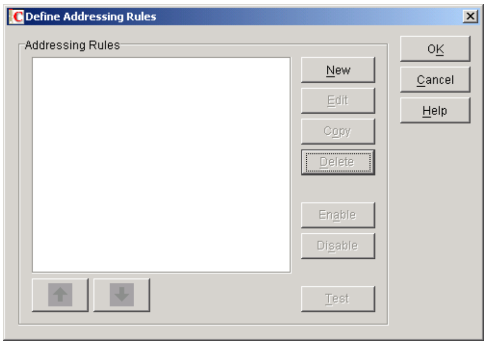
Addressing rules are created at the system level and enabled by domain.

- "Creating an Addressing Rule" on page 98
- "Enabling an Addressing Rule" on page 99

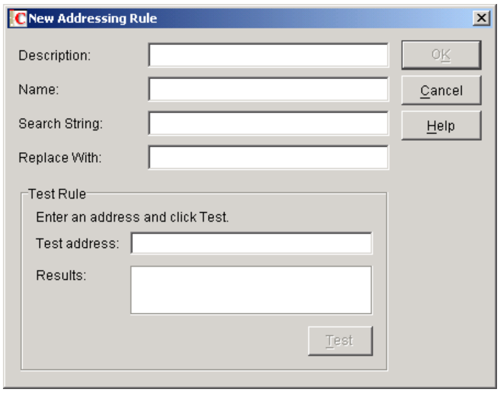
If you are using Internet-style addressing (see Chapter , "Internet-Style Addressing," on page 87), any addressing rules that include an @ in the search string and a colon (:) in the replacement string is ignored.

Creating an Addressing Rule

1 In ConsoleOne®, click the Tools menu > GroupWise System Operations > Addressing Rules.



2 Click New to display the New Addressing Rule dialog box.



3 Fill in the following fields:

Description: Enter a short description for the rule. The description is what appears when the rule is listed in the Addressing Rules dialog box.

Name: Enter the name you want to use for the rule.

Search String: Enter the text string that determines which addresses the rule is applied to. You can use an asterisk as a wildcard to represent one or more characters. For example, if you want the rule to apply to all addresses with JSmith as the userID, enter jsmith.*.* (the first asterisk represents the post office and the second represents the domain).

Replace With: Enter the replacement text. You can use variables (%1, %2, and so forth) to reference the wildcard text used in the search string. For example, if you use two wildcards in the search string, you could use two variables (%1 and %2) to insert the matched wildcard text into the replacement string. %1 (replace string 1) replaces the first wildcard in the search string, %2 replaces the second wildcard, and so on. The replacement variables must be placed in the string according to the order required for the explicit address, not according to their numerical order (for example, %2 could come before %1).

Using the jsmith.*.* example, assume that you want to replace jsmith with jjones. You would enter jjones.%1.%2. The resulting addressing would include the same post office and domain but a different userID.

4 If desired, you can test the rule on an address. To do so, enter an address in the Test Address dialog box (the address does not have to be real) > click Test to see the results.

5 Click OK to add the rule to the list.

The rule is automatically enabled, which means that it is available for use. To apply it to a domain, however, you need to enable it in the domain. For instructions, see "Enabling an Addressing Rule" on page 99.

6 If necessary, select the rule, then use the up-arrow and down-arrow to move the rule to the position in which you want it executed.

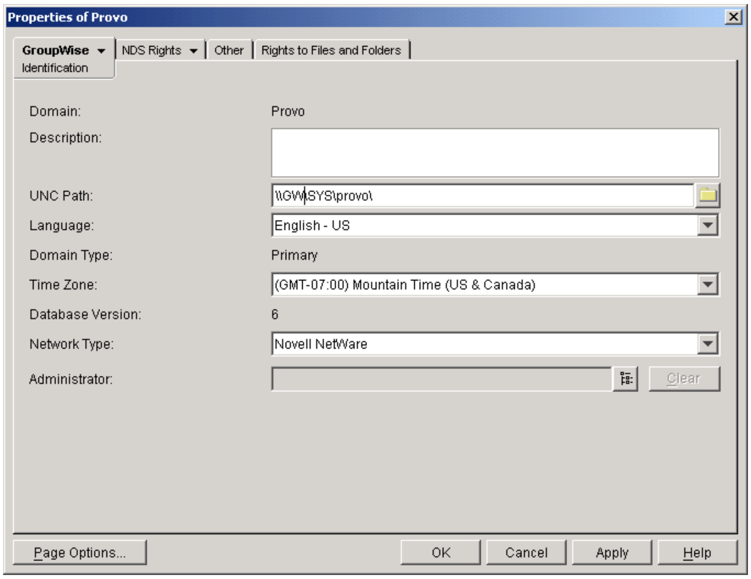
Addressing rules are executed in the order they are listed. When an addressing rule is applied to an address, no further addressing rules are applied.

7 When you are finished creating rules, click OK to close the Define Addressing Rules dialog box.

Enabling an Addressing Rule

After you create an addressing rule, you need to enable it in the domains where you want it applied.

1 In ConsoleOne, right-click the Domain object, then click Properties.



Domain: Provo

Description:

UNC Path: \\GW\SYS\provo\

Language: English - US

Domain Type: Primary

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

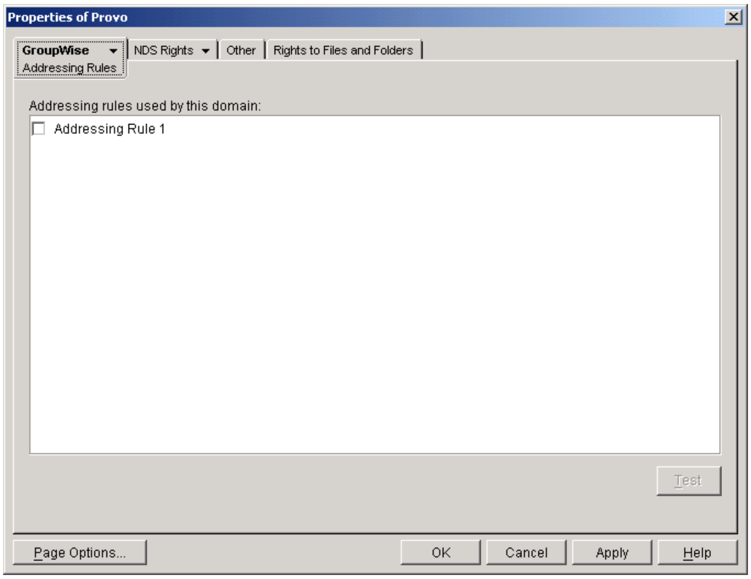
Database Version: 6

Network Type: Novell NetWare

Administrator:

2 Click GroupWise > Addressing Rules.

The list displays all addressing rules that have been made available in the system. However, an addressing rule does not apply to the domain until you enable it.



Addressing rules used by this domain:

□ Addressing Rule 1

3 Click the check box in front of an addressing rule to enable it.

4 When you are finished enabling rules, click OK to save your changes.

Wildcard Addressing

Wildcard addressing enables users to send items to all users in a post office, domain, GroupWise® system, or connected GroupWise system by inserting asterisks (*) as wildcards in e-mail addresses.

You can limit wildcard addressing to a specific level (post office, domain, system) or allow unlimited wildcard addressing. The default is to limit the wildcard addressing to post office only, meaning that a user can use wild card addressing to send to all users on his or her post office only. You can change the default for individual users, post offices, or domains.

When using wildcard addressing, the sender only sees whether the item was delivered to a domain, post office, or system (by viewing the item's properties). The properties do not show the individual usernames or additional statuses. Recipients can reply to the sender only. Reply to All is unavailable.

- "Setting Wildcard Addressing Levels" on page 100
- "Wildcard Addressing Syntax" on page 102

Wildcard addressing cannot be used for assigning shared folders or shared address books, granting proxy rights, performing busy searches, or sending routing slips.

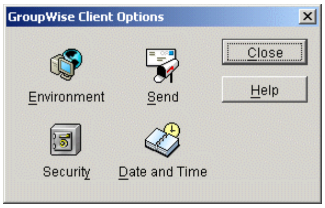
Setting Wildcard Addressing Levels

By default, wildcard addressing is enabled at the post office level for all users in your GroupWise system. You can change the level (post office, domain, or system) or disable wildcard addressing.

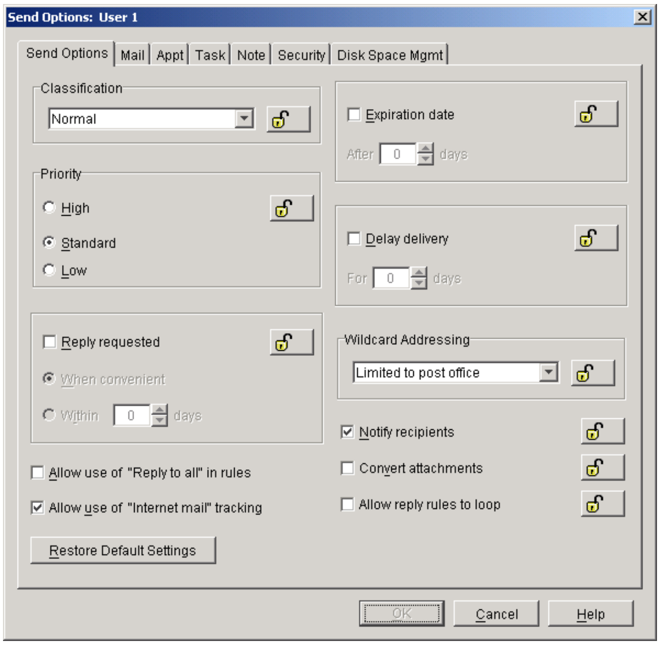
Wildcard addressing levels can be applied to a single user, to all users in a post office, or to all users in a domain.

To set wildcard addressing defaults:

1. In ConsoleOne®, select a Domain, Post Office, or User object.
2. Click the Tools menu > GroupWise Utilities > Client Options to display the GroupWise Client Options dialog box.



3. Click Send to display the Send Options dialog box.



Classification: Normal

Priority: ○ High ● Standard ○ Low

□ Reply requested
● When convenient
○ Within 0 days

□ Allow use of "Reply to all" in rules

☑ Allow use of "Internet mail" tracking

□ Expiration date
After 0 days

□ Delay delivery
For 0 days

Wildcard Addressing: Limited to post office

☑ Notify recipients

□ Convert attachments

□ Allow reply rules to loop

4. In the Wildcard Addressing list, select from the following options:
   - **Not Allowed:** Select this option to disable wildcard addressing.
   - **Limited to Post Office (Default):** Select this option to limit wildcard addressing to the user's post office. The user can use wildcard addressing to send items to users in his or her post office only.
   - **Limited to Domain:** Select this option to limit wildcard addressing to the user's domain. The user can use wildcard addressing to send items to users in his or her domain only.
   - **Limited to System:** Select this option to limit wildcard addressing to the user's GroupWise system. The user can use wildcard addressing to send items to all users in his or her system only. This excludes external users (users from other systems) who have been added to your GroupWise address book.
   - **Unlimited:** Select this option to allow unlimited use of wildcard addressing. The user can use wildcard addressing to send to all users (including external users and non-visible users) defined in the GroupWise address book.
5. Click OK to save the changes.

Wildcard Addressing Syntax

The following table shows the syntax that must be used when using wildcard addressing to send items.

WildCard Addressing Setting	To send an item to...	Type in the To field...
Limited to Post Office	All users in your post office	*
Limited to Domain	All users in your post office	*
	All users in your domain	*.*
	All users in another post office in your domain	**.post_office*
Limited to System	All users in your post office	*
	All users in your domain	*.*
	All users in another post office in your domain	**.post_office*
	All users in a post office in another domain	*.*post_office.domain*
	All users in another domain	*.*domain*
	All users in your GroupWise system	*.*.*
Unlimited	All users in your post office	*
	All users in your domain	*.*
	All users in a different post office in your domain	**.post_office*
	All users in a post office in another domain. You can also use this for external post offices and external domains.	*.*post_office.domain*
	All users in a another domain. You can also use this for external domains.	*.*domain*
	All users in the GroupWise address book (all users in the same system, all external users, and all non-visible users)	*.*.*

7 Multilingual GroupWise Systems

GroupWise® is a multilingual e-mail product that meets the needs of users around the world. The following sections provide guidance if your GroupWise system includes users that speak a variety of languages:

- "Client Languages" on page 103
- "Administration Languages" on page 104
- "International Character Considerations" on page 104
- "Multi-Language Workstations" on page 105

Client Languages

You can run the GroupWise client in the following languages:

- Arabic
- Czech
- Chinese - Simplified
- Chinese - Traditional
- Danish
- Dutch
- English
- Finnish
- French
- German
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Russian
- Spanish
- Swedish

Users can select the languages they want when they install the GroupWise client. If users have access to the GroupWise client media, they can choose from all languages. If users are installing from a software distribution directory, they can choose from the languages you installed in the software distribution directory, as described in "GroupWise Languages" in "Installing a Basic GroupWise System" in the *GroupWise 6.5 Installation Guide*. The maximum disk space required to store all the GroupWise software components for one language is approximately 500 MB.

By default, the GroupWise client starts in the language of the operating system, if it is available. If the operating system language is not available, the next default language is English. When starting the GroupWise client, you can use the /l startup switch to override the English default and select an interface language from those that have been installed.

The online help available in the GroupWise clients is provided in all languages into which the client software is translated. The GroupWise client user guides available from the GroupWise clients and on the GroupWise Documentation Web site are translated only into the administration languages. If you try to access a user guide from a client that is running in a language into which the user guide has not been translated, you can select any of the available languages.

Administration Languages

You can run the GroupWise Installation program, administer your GroupWise system in ConsoleOne®, and run the GroupWise agents in the following languages:

English

French

German

Spanish

Portuguese

All available administration languages are automatically installed.

When you select a language for a domain, it determines the sorting order for items in the GroupWise Address Book. This language becomes the default for post offices that belong to the domain. You can override the domain language at the post office level if necessary.

For example, if you set the domain and post office language to English-US, the Address Book items are sorted according to English-US sort order rules. This is true even if some users in the post office are running non-English-US GroupWise clients such as German or Japanese. Their client interface and Help files are in German or Japanese, but the sort order is according to English-US standards.

By default, the agents start in the language selected for the domain. If that language has not been installed, the agents start in the language used by the operating system. If that language has not been installed, the agents start in English-US.

The POA also includes language-specific files in all client languages so that information returned from the POA to the GroupWise client, such as message status and undeliverable messages, is displayed in the language of the GroupWise client rather than the language in which the POA interface is being displayed.

International Character Considerations

GroupWise client users have complete flexibility in the characters they use in composing messages. Accented characters used by various European languages and double-byte characters used by various Asian and Middle Eastern languages are all acceptable in the GroupWise client and can even be combined in the same message text.

As an administrator, the only limitation you need to be aware of is that double-byte Asian and Middle Eastern characters should not be used in directory names and filenames within your GroupWise system. This limitation is based on operating system capabilities. You should also not use double-byte characters in passwords. You are free to use double-byte characters in GroupWise usernames, domain names, post offices names, and so on.

Multi-Language Workstations

If GroupWise users receive messages in multiple languages, their workstations need to be configured to handle the character sets used by these languages.

On Windows XP:

1. From the Control Panel, double-click Regional and Language Options, then click Languages.
2. If you receive messages in Arabic, Hebrew, or other complex languages, select Install Files for Complex Script and Right-to-Left Languages.
3. If you receive messages in Chinese, Japanese, or other similar languages, select Install Files for East Asian Languages
4. Click OK to install the required language files.

On Windows 2000:

1. From the Control Panel, double-click Regional Options.
2. Select the languages you want to use on the workstation, then click OK to install the required language files.

On Linux and Macintosh workstations, if users see the correct characters at the operating system and desktop levels, they see the correct characters in GroupWise as well.

II Domains

8 Creating a New Domain

As your GroupWise® system grows, you might need to add new domains.

- "Understanding the Purpose of Domains" on page 109
- "Planning a New Domain" on page 110
- "Setting Up the New Domain" on page 118
- "What's Next" on page 121

IMPORTANT: If you are creating a new domain in a clustered GroupWise system, see the appropriate section of the GroupWise 6.5 Interoperability Guide before you create the domain:

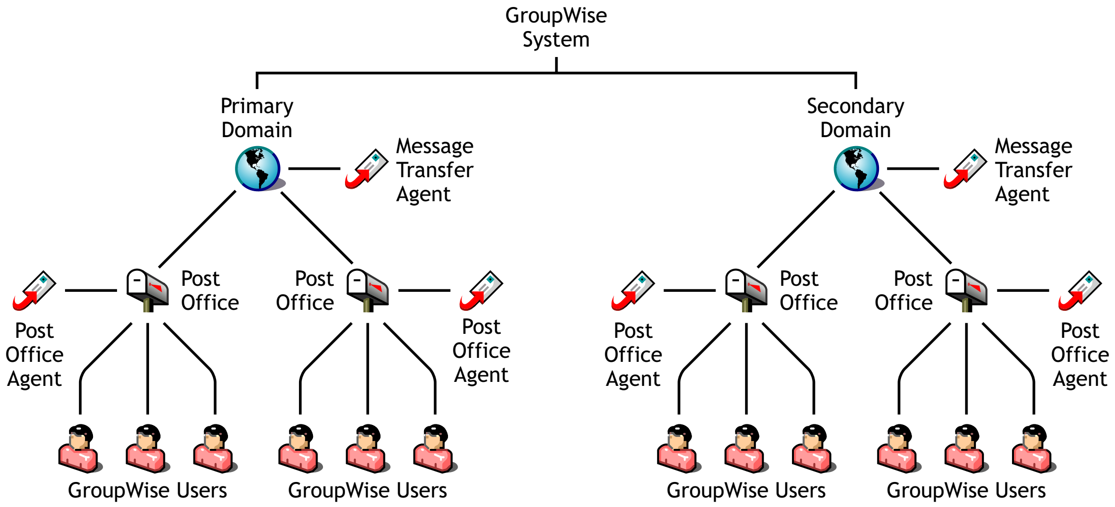
- "Setting Up a Domain and Post Office in a Novell Cluster" in "Novell Cluster Services"
- "Setting Up a Domain and Post Office in a Microsoft Cluster" in "Microsoft Clustering Services"

Understanding the Purpose of Domains

The domain functions as the main administrative unit for your GroupWise system. Each GroupWise system has one primary domain, which was created when you first installed GroupWise. All other domains that you add are secondary domains.

The domain serves as a logical grouping of one or more post offices and is used for addressing and routing messages. Each GroupWise user has a GroupWise address that consists of a user ID, the user's post office name, the GroupWise domain name, and, optionally, an Internet domain name.

The following diagram illustrates the logical organization of a GroupWise system with multiple domains and post offices. All of the objects under the domain belong to that domain. All of the objects under a post office belong to that post office.



Messages are moved from user to user through your GroupWise system by the GroupWise agents. As illustrated above, each domain must have a Message Transfer Agent (MTA) running for it. The MTA transfers messages between domains and between post offices in the same domain. Each post office must have at least one Post Office Agent (POA) running for it. The POA delivers messages to users' mailboxes and performs a variety of post office and mailbox maintenance activities.

When you add a new domain to your GroupWise system, links define how messages are routed from one domain to another. When you add the first secondary domain, the links between the primary and secondary domains are very simple. As the number of domains grows, the links among them can become quite complex. Links are discussed in detail in Chapter 10, "Managing the Links between Domains and Post Offices," on page 131.

Physically, a domain consists of a set of directories that house all the information stored in the domain. To view the structure of a domain directory, see "Domain Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. The domain directory does not contain mailboxes or messages, but it does contain other vital information. For an overview, see "Information Stored in the Domain" on page 558. Domain directories can be located on NetWare, Linux, and Windows servers.

Planning a New Domain

After you have your basic GroupWise system up and running, you might need to expand it by adding one or more domains. The GroupWise architecture lets you create a simple, single domain system, or a complex system that links dozens of domains across a campus, a city, or around the world.

This section provides the information you need in order to decide when, where, and how to set up a new domain. The "Domain Worksheet" on page 122 lists all the information you need. You should print the worksheet and fill it out as you complete the tasks listed below.

- "Determining When to Add a New Domain" on page 111
- "Deciding Who Will Administer the New Domain" on page 111
- "Planning Post Offices in the New Domain" on page 112
- "Determining the Context for the Domain Object" on page 112
- "Choosing the Domain Name" on page 114
- "Deciding Where to Create the Domain Directory" on page 114
- "Deciding Where to Install the Agent Software" on page 115
- "Deciding How to Link the New Domain" on page 117
- "Selecting the Domain Language" on page 118
- "Selecting the Domain Time Zone" on page 118

After you have completed the tasks and filled out the "Domain Worksheet" on page 122, you are ready to continue with "Setting Up the New Domain" on page 118.

Determining When to Add a New Domain

How do you know when you should add a domain? The answer to this depends on your administration policies and on physical and logical network organization.

Although a single domain can contain as many post offices and users as you want to add, there are some conditions that indicate the need for a new domain:

- **Administrative Convenience:** To spread out the administrative workload, you can create one or more new domains with their own administrators. Each new domain can be managed by a different administrator as long as each administrator has sufficient rights to connect to it and write to the domain directory.
- **Remote Sites:** If communication between servers is slow, or if you have remote sites, you can add a new domain to minimize mail traffic between the servers. For example, if you have locations in three separate cities, you might have an organization that represents each location. You could then create a domain in each organization. You could administer all of the domains from one location or you could assign a different administrator for each one.
- **Demand on the MTA:** Each domain has its own MTA that routes messages between post offices within its domain. If your current domain has many post offices that are placing a heavy workload on the MTA, you might want to create another domain to handle additional post offices.
- **Multiple eDirectory Trees:** All of the objects that are logically subordinate to a GroupWise domain must be in the same Novell® eDirectory™ tree as the domain. If you have users in other eDirectory trees that need GroupWise accounts, you must create secondary domains and post offices in each tree.

Deciding Who Will Administer the New Domain

Any user who is an Admin equivalent can administer GroupWise. We recommend that whoever creates the new domain should be an Admin equivalent so that he or she has the necessary rights to create objects and directories. You can then assign a different user as a domain administrator and limit rights to other objects if necessary. For more information, see Chapter 84, "GroupWise Administrator Rights," on page 1053.

Depending upon the size, complexity, and layout of your eDirectory tree, you might choose a centralized administration model with one person administering both eDirectory and GroupWise, or you might choose a distributed administration model with the administration workload shared by two or more individuals. With a distributed administration model, each administrator obtains rights to the GroupWise objects and directory structures over which he or she has jurisdiction. If you want to restrict access to some network operations or to certain domains, you can limit access rights to domains the user should not administer.

The user assigned as the administrator must be able to create or modify objects in the domain and will receive an e-mail message whenever an agent encounters a problem. You can designate yourself, one or more other users, or a distribution list as an administrator.

WORKSHEET

Under Item 10: Domain Administrator, enter the ID of the user or distribution list that will administer this domain.

The items in the worksheet are listed in the order you will enter them when setting up your domain. This planning section does not follow the same order as the worksheet, but all worksheet items are covered.

Planning Post Offices in the New Domain

Before adding the new domain, you should plan the post offices that you want to belong to the domain. You should consider the following issues when planning post offices.

- **Physical Organization:** If your network spans several sites, you might want to create post offices (if not domains) at each physical location. This reduces the demands on long-distance network links.
- **Logical Organization:** Grouping users who frequently send messages to each other is faster and generates less network traffic than if messages travel between different post offices and domains.
- **Number of Users:** A typical post office can serve from 1000 to 2500 users, depending on its configuration. Larger post offices are possible, but grouping similar users might be preferable.
- **Demand on the POA:** Each post office has at least one POA that delivers messages to users' mailboxes and performs other post office maintenance tasks. It is possible to run multiple POAs, located on different servers, for the same post office, or you might prefer to create multiple post offices.

For more details, see "Planning a New Post Office" on page 148.

Determining the Context for the Domain Object

When deciding where to place the new Domain object in the eDirectory tree, you should consider how you can most easily administer GroupWise and how the domain and its associated post offices fit into the logical organization of your eDirectory tree.

Domains and their associated objects, including Post Offices, Users, Resources, and Distribution Lists, must be located in the same eDirectory tree. If you have multiple trees, you must create a separate domain in each tree. The domains can all belong to the same GroupWise system.

You can place the domain in any context in an eDirectory tree. The following diagrams provide some examples of how domains can be placed in the eDirectory tree:

- "GroupWise Objects Reflect Physical Locations" on page 112
- "GroupWise Objects Reflect Company Organization" on page 113
- "GroupWise Objects Are Grouped with Servers" on page 113
- "GroupWise Objects Are Located in a Separate GroupWise Container" on page 113

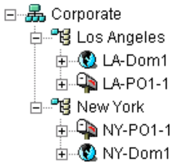
WORKSHEET

Under Item 1: Tree Name, specify the name of the eDirectory tree where you plan to create the new domain.

Under Item 2: eDirectory Container, specify the name of the eDirectory container where you plan to create the new domain.

GroupWise Objects Reflect Physical Locations

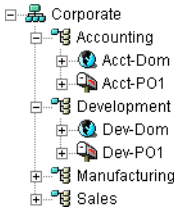
The GroupWise system below focuses on the physical layout of the company. Because most mail traffic is probably generated by users in the same location, the mail traffic across the WAN is minimized. An organizational unit was created for each site. A domain was created under each organizational unit, corresponding to the city. The sites can be administered centrally or at each site. Administrator rights can be assigned at the domain level.



- Corporate
  - Los Angeles
    - LA-Dom1
    - LA-PO1-1
  - New York
    - NY-PO1-1
    - NY-Dom1

GroupWise Objects Reflect Company Organization

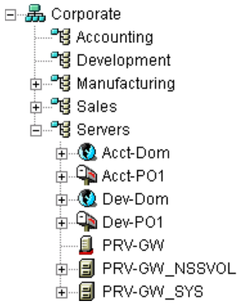
The following GroupWise system focuses on departmental organization, as does the eDirectory tree. GroupWise domains and post offices parallel eDirectory organizational units, placing the domains and post offices within the organizational units containing the users that will belong to them.



- Corporate
  - Accounting
    - Acct-Dom
    - Acct-PO1
  - Development
    - Dev-Dom
    - Dev-PO1
  - Manufacturing
  - Sales

GroupWise Objects Are Grouped with Servers

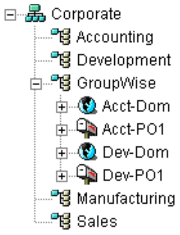
Because domains and post offices have directory structures on network servers, you could also choose to place the Domain and Post Office objects in the same context as the servers where the directories will reside, as shown in the following example.



- Corporate
  - Accounting
  - Development
  - Manufacturing
  - Sales
  - Servers
    - Acct-Dom
    - Acct-PO1
    - Dev-Dom
    - Dev-PO1
    - PRV-GW
    - PRV-GW_NSSVOL
    - PRV-GW_SYS

GroupWise Objects Are Located in a Separate GroupWise Container

Domains and post offices can also be created in their own organizational unit. Administratively, this approach makes it easier to restrict a GroupWise administrator's object and property rights to GroupWise objects only. For information about GroupWise Administrator rights, see "Deciding Who Will Administer the New Domain" on page 111.



- Corporate
  - Accounting
  - Development
  - GroupWise
    - Acct-Dom
    - Acct-PO1
    - Dev-Dom
    - Dev-PO1
  - Manufacturing
  - Sales

Choosing the Domain Name

The domain requires a unique name. The name is used as the Domain object's name in eDirectory. It is also used for addressing and routing purposes within GroupWise, and might appear in the GroupWise Address Book.

The domain name can reflect a location, company name or branch name, or some other element that makes sense for your organization. For example, you might want the domain name to be the location (for example, Provo) while the post office name is one of the company's departments (for example, Research). Name the new domain carefully. After it is created, the name cannot be changed.

The domain name can consist of one or more words. Use underscores (_) rather than spaces as separators between words to facilitate addressing across the Internet. Do not use any of the following invalid characters in the domain name:

ASCII characters 0-13

Asterisk *

At sign @

Braces { }

Colon :

Comma ,

Double quote "

Extended characters

Parentheses ( )

Period .

WORKSHEET

Under Item 3: Domain Name, specify the domain name.

Under Item 8: Domain Description, provide a description for the new domain.

Deciding Where to Create the Domain Directory

Logically, the Domain object resides in eDirectory and is administered through ConsoleOne®. Physically, the domain has a directory structure for databases, message queues, and other files. The domain directory structure can be created on NetWare® servers (NetWare 6.*x*, NetWare 5.*x*, NetWare 4.2, or NetWare 3.12), Linux servers (SUSE Standard or Enterprise Server 8, Red Hat* Enterprise Linux 3 ES or AS), or Windows servers (Windows 2000 or Windows NT*). The server where you create the domain directory structure can be in the same tree as the Domain object or in another tree.

Many different configurations are possible. When deciding where to create the domain directory, you should consider the following.

- **Domain Directory Space Requirements:** The domain directory requires less than 10 MB of free disk space. However, this requirement could increase as your system grows.
- **Network Access by the MTA:** If the MTA is not installed on the same server with the domain directory, the MTA must have direct network access (mapped drive or file system mount) to the domain directory and, depending on link configuration, to the post office directories. This issue is discussed in detail in "Deciding Where to Install the Agent Software" on page 115.
- **Security from User Access:** Users never need access to the domain directory so you should create it in a location you can easily secure; otherwise, you could have files inadvertently moved or deleted.

Choose an empty directory for the new domain. If you want, the directory can reflect the name of the domain, for example, res_dev for the Research and Development domain. On NetWare and Windows, use a maximum of 8 characters in the directory name. On Linux, use only lowercase characters in the directory name.

Choose the name and path carefully. After the domain directory is created, it is difficult to rename it. If the directory you specify does not exist, it will be created when you create the domain. Do not create the domain directory under another domain or post office directory.

WORKSHEET

Under Item 4: Domain Database Location, enter the full path for the domain directory.

Under Item 9: Network Type, enter the type of network in use at that location.

Deciding Where to Install the Agent Software

You must run a new instance of the MTA for each new domain. To review the functions of the MTA for the domain, see "Role of the Message Transfer Agent" on page 559. For complete installation instructions and system requirements, see "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

When planning the installation of the MTA, you need to consider how the new domain links to existing domains and how the new domain will link to its post offices. For an overview of link configuration, see Chapter 10, "Managing the Links between Domains and Post Offices," on page 131.

The MTA requires direct network access to the domain directory and, depending on the link configuration, to each post office directory. Consider the following alternatives when selecting a location for the MTA relative to the domain and its post offices:

- "MTA Access to the New Domain: Local vs. Remote" on page 115
- "MTA Access to New Post Offices: Mapped and UNC Links vs. TCP/IP Links" on page 116
- "Cross-Platform Access Issues" on page 117

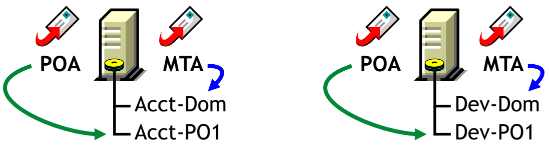
WORKSHEET

Under Item 11: Agent Location, indicate whether you plan to run the MTA on the same server where the domain directory is located, or on a different server.

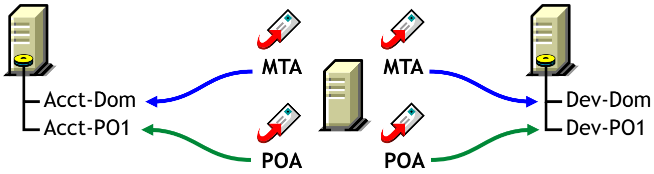
Under Item 12: Agent Platform, enter the platform of the server where the MTA will run (NetWare, Linux, or Windows).

MTA Access to the New Domain: Local vs. Remote

Running the MTA locally on the same server where the domain and post offices reside simplifies network connections (no login is required), reduces network traffic, and protects database integrity. In the following diagram, the agent software is installed on the same server where the domain and post office reside.



Running the MTA on a remote server allows you to place the heaviest processing load on your highest performing server. In the following diagram, the agent software is installed on a different server from where the domains and post offices reside.

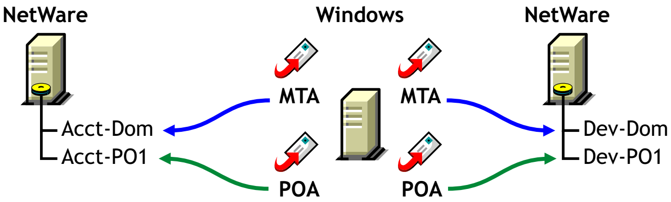


When you run the MTA on a different server from where its directory structures and databases are located, you need to provide adequate access.

- If the NetWare® MTA needs direct network access to another NetWare server, you must add the /dn switch or the /user and /password switches to the MTA startup file to provide authentication information.
- If the Linux MTA needs direct network access to another Linux server, you must mount the file system where the domain is located before you start the Linux MTA.
- If the Windows MTA needs direct network access to another Windows server, you must map a drive to the other server before you start the Windows MTA.

MTA Access to New Post Offices: Mapped and UNC Links vs. TCP/IP Links

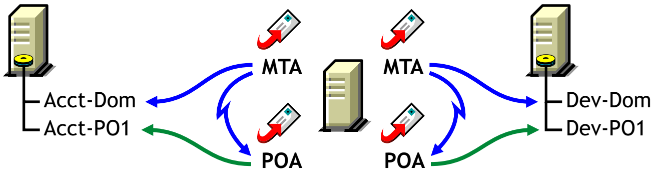
If the new domain will include multiple post offices, the post offices will probably reside on different servers from where the domain is located. If you plan to use mapped or UNC links between the domain and its post offices, the MTA requires the same access to the post office directories as it requires to the domain directory.



- If the NetWare MTA needs access to a post office on another NetWare server, you must add the /dn switch or the /user and /password switches to the MTA startup file to provide authentication information.
- If the Windows MTA needs access to a post office on another Windows server, you must map a drive to the other server before you start the Windows MTA.

NOTE: The Linux MTA requires TCP/IP links to the POA.

To avoid these direct network access requirements between the MTA and its post offices, you can use TCP/IP links between the domain and its post offices.

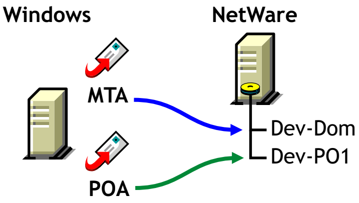


When using TCP/IP links, the MTA does not write message files into message queues in the post office directory structure. Instead, the MTA communicates the information to the POA by way of TCP/IP and then the POA uses its direct network access to write the information.

Cross-Platform Access Issues

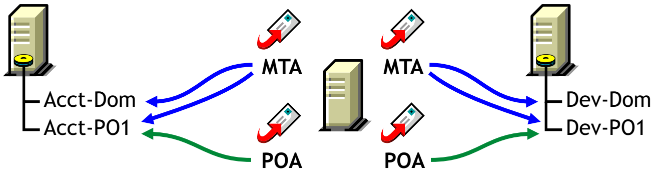
In most cases, it is most efficient if you match the MTA platform with the network operating system where the domain resides. For example, if you create a new domain on a NetWare server, use the NetWare MTA.

If you decide not to run the MTA on the same platform as the domain, the MTA must still have direct network access to the domain directory so that it can write to the domain database (wpdomain.db). For example, you could set up the new domain on a NetWare server and run the Windows MTA on an Windows server to service it.



However, the NetWare MTA could not service a domain located on an Windows server because Windows does not support the required cross-platform connection.

If you are using mapped or UNC links to post offices, the MTA must also have direct network access to the post office directories so that it can write messages files into the post office message queues. You could, for example, run the agents on an Windows server while domains and post offices were located on NetWare servers.



Again, the opposite combination of NetWare agents servicing domains and post offices on Windows servers is not an option because Windows does not support the required cross-platform connection.

To avoid these cross-platform access issues, use TCP/IP links between a domain and its post offices.

For more detailed information, see "Cross-Platform Issues between Domains and Post Offices" on page 561.

Deciding How to Link the New Domain

Domain links tell the MTAs how to route messages between domains. Properly configured links optimize message flow throughout your GroupWise system. For a review of link types, see "Domain-to-Domain Links" on page 131.

When you create the new domain, you link it to one existing domain. By default, this link is a direct link using TCP/IP as the link protocol, which means the new domain's MTA communicates with the existing domain's MTA through TCP/IP. If desired, you can configure the direct link to use a UNC path as the link protocol, which means the new domain's MTA transfers information to and from the existing domain by accessing the existing domain's directory

WORKSHEET

Under Item 7: Link to Domain, specify the existing domain that you want to link the new domain to, then specify the link protocol (TCP/IP or UNC path).

After you create the new domain, you can configure links to additional domains as needed. See "Using the Link Configuration Tool" on page 136.

Selecting the Domain Language

The domain language determines how times, dates, and numbers are displayed in the GroupWise client and determines the sorting rules for items in the GroupWise Address Book.

WORKSHEET

Under Item 5: Domain Language, specify the domain language.

Selecting the Domain Time Zone

When a message is sent from a user in one time zone to a user in another time zone, GroupWise adjusts the message's time so that it is correct for the recipient's time zone. For example, if a user in New York (GMT -05:00, Eastern Time) schedules a user in Los Angeles (GMT -08:00, Pacific Time) for a conference call at 4:00 p.m. Eastern Time, the appointment is scheduled in the Los Angeles user's calendar at 1:00 p.m. Pacific Time.

The domain time zone becomes the default time zone for each post office in the domain.

WORKSHEET

Under Item 6: Domain Time Zone, enter the time zone.

Setting Up the New Domain

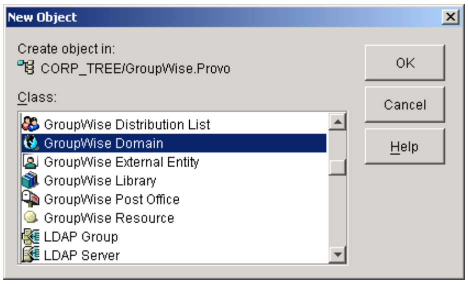
You should have already reviewed "Planning a New Domain" on page 110 and filled out the "Domain Worksheet" on page 122. Complete the following tasks to create the new domain.

- "Creating the New Domain" on page 119
- "Configuring the MTA for the New Domain" on page 120
- "Installing and Starting the New MTA" on page 121

Creating the New Domain

1 Make sure you are logged in to the tree where you want to create the domain (worksheet item 1).

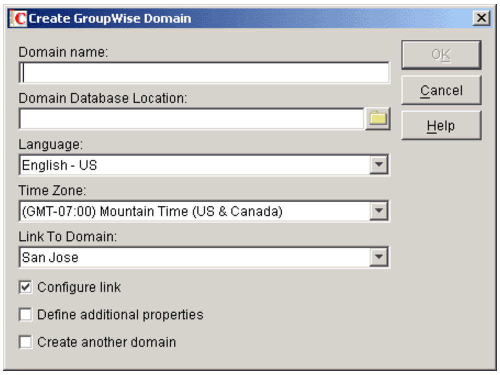
2 In ConsoleOne, browse to and right-click the eDirectory container where you want to create the domain (worksheet item 2), then click New > Object.


New Object

Create object in:
CORP_TREE/GroupWise.Provo

Class:
- GroupWise Distribution List
- GroupWise Domain
- GroupWise External Entity
- GroupWise Library
- GroupWise Post Office
- GroupWise Resource
- LDAP Group
- LDAP Server

3 Double-click GroupWise Domain, then fill in the fields in the Create GroupWise Domain dialog box (worksheet items 3 through 7).


Create GroupWise Domain

Domain name:

Domain Database Location:

Language: English - US

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

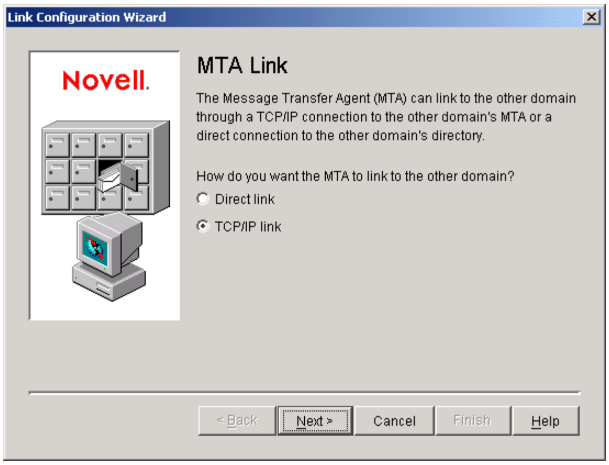
Link To Domain: San Jose

☑ Configure link

☐ Define additional properties

☐ Create another domain

4 Make sure the Configure Links and Define Additional Properties options are selected, then click OK to display the Link Configuration Wizard.


Link Configuration Wizard

MTA Link

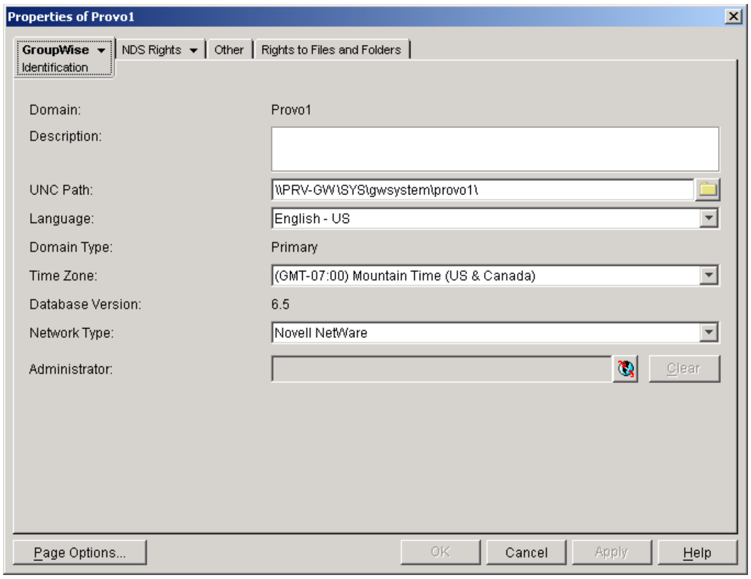
The Message Transfer Agent (MTA) can link to the other domain through a TCP/IP connection to the other domain's MTA or a direct connection to the other domain's directory.

How do you want the MTA to link to the other domain?

○ Direct link

● TCP/IP link

5 Follow the on-screen instructions to define how the new domain links to the existing domain (listed in the Link to Domain field). When you've finished defining the link, ConsoleOne creates the Domain object and displays the domain Identification page.



Properties of Provo1

Domain: Provo1

Description:

UNC Path: \\PRV-GW\SYS\gwsystem\provo1\

Language: English - US

Domain Type: Primary

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Database Version: 6.5

Network Type: Novell NetWare

Administrator:

6 Fill in the fields that have not been filled in for you (worksheet items 8 through 10).

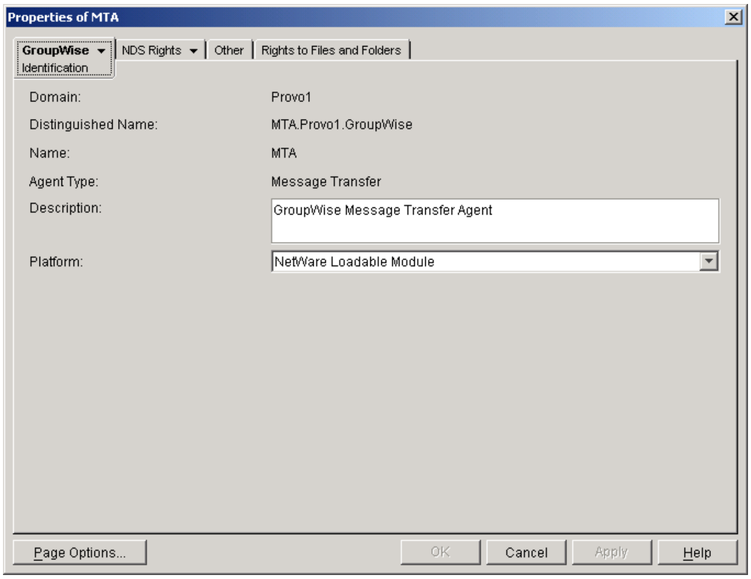
7 Click OK to save the domain information.

Configuring the MTA for the New Domain

Although there are many MTA settings, the default settings are sufficient to get your domain operational. However, there are a few important settings that you can conveniently modify before you install the agent software.

1 In ConsoleOne, double-click the new Domain object.

2 Right-click the MTA object, then click Properties to display the MTA Identification page.



Properties of MTA

Domain: Provo1

Distinguished Name: MTA.Provo1.GroupWise

Name: MTA

Agent Type: Message Transfer

Description: GroupWise Message Transfer Agent

Platform: NetWare Loadable Module

3. Enter a description for the MTA.

   This description displays on the MTA agent console as the MTA runs.

4. Select the platform where the MTA will run (worksheet item 12).
5. If you have multiple domains in your system and want to use TCP/IP to link to the other domains (worksheet item 7), follow the instructions in "Using TCP/IP Links between Domains" on page 579.
6. If you have created the domain in a clustered environment, follow the instructions in the appropriate section of the GroupWise 6.5 Interoperability Guide:
   - "Installing and Configuring the MTA and the POA in a Cluster" in "Novell Cluster Services"
   - "Installing and Configuring the MTA and the POA in a Cluster" in "Microsoft Clustering Services"
7. To ensure that user information in the new domain stays synchronized with user information in eDirectory, follow the instructions in "Using eDirectory User Synchronization" on page 598.
8. For more MTA configuration options, see "Changing MTA Configuration to Meet Domain Needs" on page 130.
9. Click OK to save the MTA configuration information.

Installing and Starting the New MTA

To install the MTA for the new domain to the location recorded under worksheet item 11, follow the instructions in "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*. For additional MTA-specific instructions, see Chapter 42, "Installing and Starting the MTA," on page 565.

Continue with What's Next.

What's Next

After you have added the new domain and started its MTA, you are ready to continue to expand and enhance your GroupWise system by:

- Adding post offices to the new domain. See "Post Offices" on page 145.
- Configuring the MTA for optimal performance. See "Message Transfer Agent" on page 555.
- Setting up GroupWise Monitor to monitor the GroupWise agents. See "Monitor" on page 901.
- Connecting domains and GroupWise systems across the Internet using the GroupWise Internet Agent. See "Internet Agent" on page 659.
- Connecting domains and GroupWise systems using gateways. For a list of gateways, see GroupWise 6.x Gateways (http://www.novell.com/documentation/gw6xgate/index.html). GroupWise 5.5 gateways can be used with GroupWise 6.*x*.

Domain Worksheet

Use this worksheet as you complete the tasks described in "Planning a New Domain" on page 110.

Item	Explanation
1) Tree Name:	Specify the name of the eDirectory tree where you want to create the secondary domain. For more information, see "Determining the Context for the Domain Object" on page 112.
2) eDirectory Container:	Specify the name of the eDirectory container where you want to create the new domain. For more information, see "Determining the Context for the Domain Object" on page 112.
3) Domain Name:	Specify a name for the new domain. Choose the name carefully. After the domain is created, it cannot be renamed. For more information, see "Choosing the Domain Name" on page 114.
4) Domain Database Location:	Specify the path for the domain directory. Choose the domain directory carefully. After it is created, it is difficult to rename. For more information, see "Deciding Where to Create the Domain Directory" on page 114.
5) Domain Language:	Specify a default language for the domain. For more information, see "Selecting the Domain Language" on page 118.
6) Domain Time Zone:	Specify the time zone where the domain is located. For more information, see "Selecting the Domain Time Zone" on page 118.
7) Link to Domain: Link Protocol: ◆ UNC path ◆ TCP/IP Address: Port:	Specify the existing domain that you want to link the new domain to, then specify the link protocol. If you select TCP/IP, enter the IP address or hostname of the server where the MTA will run and the port number that the MTA will listen on. For more information, see "Deciding How to Link the New Domain" on page 117.
8) Domain Description:	Enter a description for the domain to help you identify its function in the system.
9) Network Type:	Specify the network type in use on the server where this domain will be located. For more information, see "Deciding Where to Create the Domain Directory" on page 114.
10) Domain Administrator:	Enter the ID of the user or distribution list that will administer this domain. For more information, see "Deciding Who Will Administer the New Domain" on page 111.
11) Agent Location: ◆ MTA on the same server as the domain (local) ◆ MTA on a different server from the domain (remote)	Mark the location of the MTA relative to the domain. For more information, see "Deciding Where to Install the Agent Software" on page 115.
12) Agent Platform: ◆ NetWare MTA ◆ Linux MTA ◆ Windows MTA	Specify the platform on which you plan to run the MTA. For more information, see "Deciding Where to Install the Agent Software" on page 115.

9 Managing Domains

As your GroupWise® system grows and evolves, you might need to perform the following maintenance activities on domains:

- "Connecting to a Domain" on page 123
- "Editing Domain Properties" on page 124
- "Converting a Secondary Domain to a Primary Domain" on page 126
- "Moving a Domain" on page 127
- "Deleting a Domain" on page 128
- "Changing MTA Configuration to Meet Domain Needs" on page 130

See also Chapter 26, "Maintaining Domain and Post Office Databases," on page 345.

Connecting to a Domain

Whenever you change domain information, it is most efficient to connect directly to the domain before you begin making modifications.

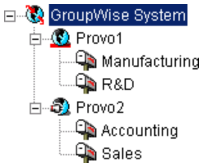
To change your domain connection:

1 In ConsoleOne® in the Console View, click Tools > GroupWise System Operations, click Select Domain, browse to and select the domain directory, then click OK.

or

In the GroupWise View, right-click the Domain object, then click Connect.

The GroupWise view identifies the domain to which you are connected by adding a plug symbol to the domain icon.

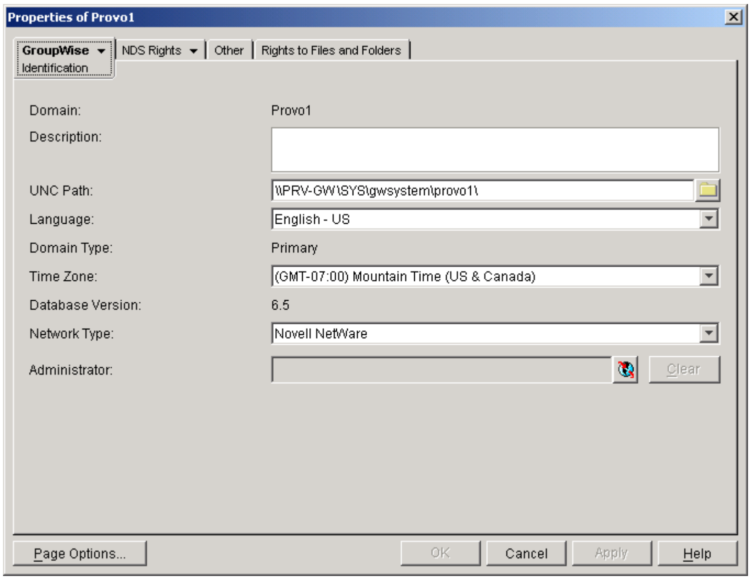


The domain marked with the red underscore is the primary domain.

Editing Domain Properties

After creating a domain, you can change some domain properties. Other domain properties cannot be changed.

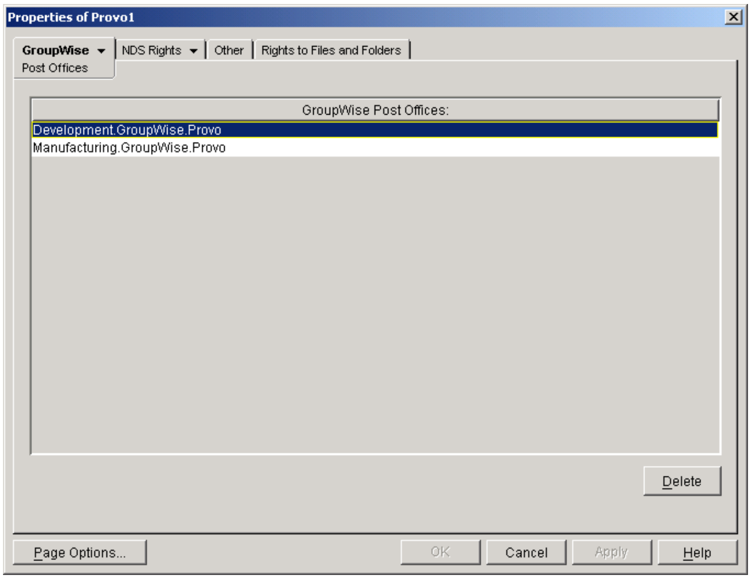
1 In ConsoleOne, browse to and right-click a Domain object, then click Properties to display the domain Identification page.



Domain: Provo1
Description:
UNC Path: \\PRV-GW\SYS\gwsystem\provo1\
Language: English - US
Domain Type: Primary
Time Zone: (GMT-07:00) Mountain Time (US & Canada)
Database Version: 6.5
Network Type: Novell NetWare
Administrator:

2 Change editable fields as needed. For information about individual fields, see "Planning a New Domain" on page 110 or use online help when editing the domain information.

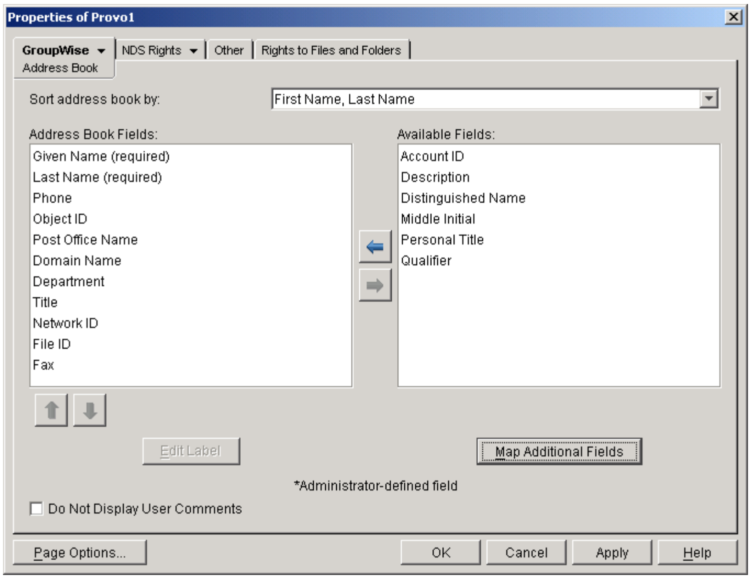
3 Click GroupWise > Post Offices to display the Post Offices page.



GroupWise Post Offices:
Development.GroupWise.Provo
Manufacturing.GroupWise.Provo

All post offices in the domain are listed, no matter where their Novell® eDirectory™ objects are placed in the tree. This is a convenient place to delete post offices from the domain.

4 Click GroupWise > Address Book to display the Address Book page.



Sort address book by: First Name, Last Name

Address Book Fields:

Given Name (required)
Last Name (required)
Phone
Object ID
Post Office Name
Domain Name
Department
Title
Network ID
File ID
Fax

Available Fields:

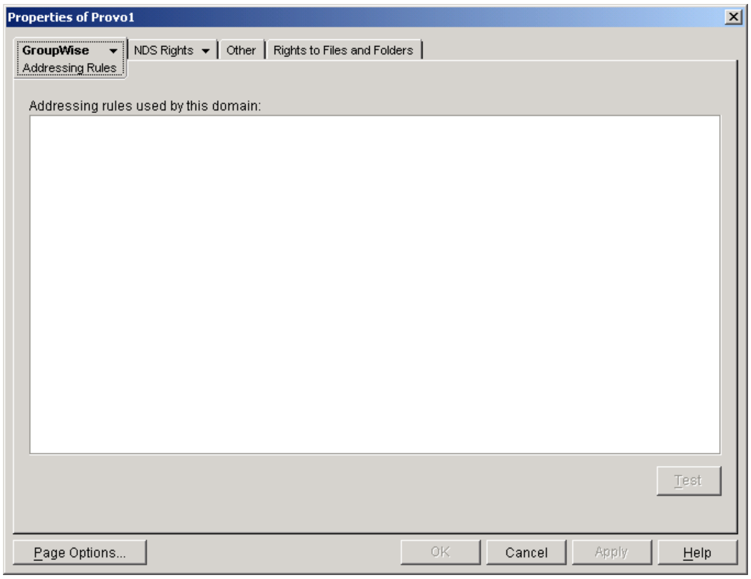
Account ID
Description
Distinguished Name
Middle Initial
Personal Title
Qualifier

*Administrator-defined field

□ Do Not Display User Comments

5 Use this page to configure the Address Book to control how it appears to GroupWise client users in all post offices in the domain. See Chapter , "Address Book," on page 81 for more information.

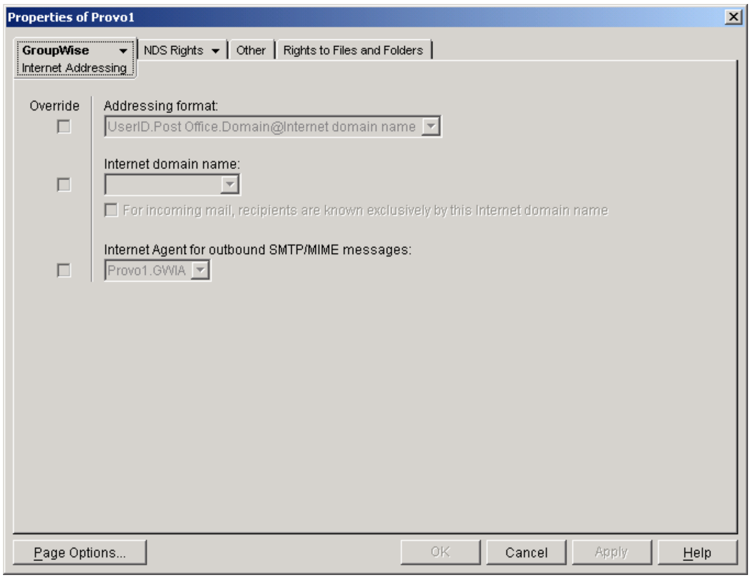
6 Click GroupWise > Addressing Rules to display the Addressing Rules page.



Addressing rules used by this domain:

This page lists all addressing rules that have been set up for the domain. See Chapter , "Addressing Rules," on page 97 for more information.

7 Click GroupWise > Internet Addressing to display the Internet Addressing page.



Override

□ Addressing format: UserID.Post Office.Domain@Internet domain name

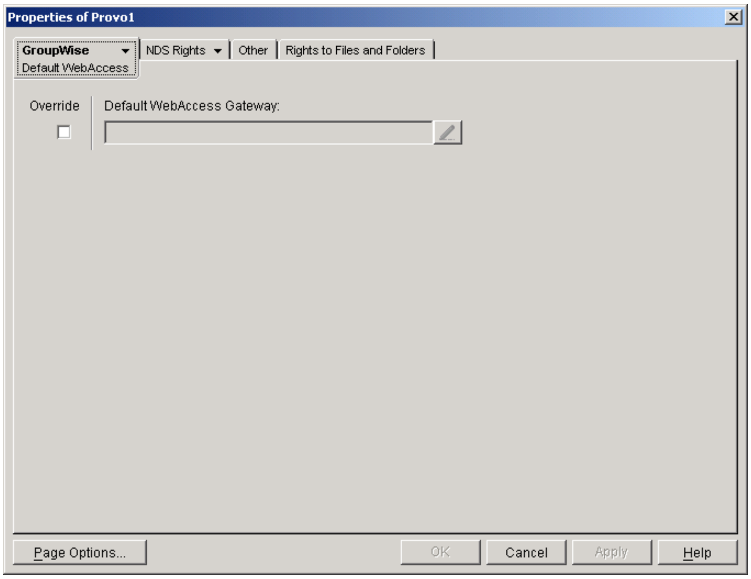
□ Internet domain name:

□ For incoming mail, recipients are known exclusively by this Internet domain name

□ Internet Agent for outbound SMTP/MIME messages: Provo1.GWIA

Use this page to override any Internet addressing settings established at the system level. See Chapter , "Internet-Style Addressing," on page 87 for more information.

8 Click GroupWise > Default WebAccess to display the Default WebAccess page.



Override

□ Default WebAccess Gateway:

Use this page to designate the default WebAccess Agent (gateway) for the domain. See "WebAccess" on page 803 for more information.

9 Click OK to save the new domain settings.

Converting a Secondary Domain to a Primary Domain

You can change which domain is primary if it becomes more convenient to administer the primary domain from a different location. You can, however, have only one primary domain at a time. When you convert a secondary domain to primary, the old primary domain becomes a secondary domain.

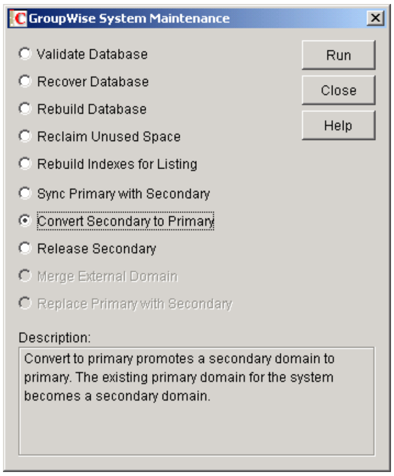
To convert a secondary domain to primary:

1 In ConsoleOne, connect to the primary domain, as described in "Connecting to a Domain" on page 123.

2 Make sure there are no pending operations for the current primary domain. See "Pending Operations" on page 51.

3 In ConsoleOne, browse to and select the secondary domain you want to convert.

4 Click Tools > GroupWise Utilities > System Maintenance.

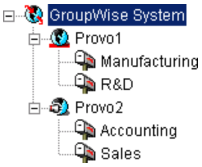

GroupWise System Maintenance
○ Validate Database
○ Recover Database
○ Rebuild Database
○ Reclaim Unused Space
○ Rebuild Indexes for Listing
○ Sync Primary with Secondary
● Convert Secondary to Primary
○ Release Secondary
○ Merge External Domain
○ Replace Primary with Secondary
Run
Close
Help
Description:

Convert to primary promotes a secondary domain to primary. The existing primary domain for the system becomes a secondary domain.

5 Click Convert Secondary to Primary.

6 Enter the path to the secondary domain database, then click OK.

The GroupWise View in ConsoleOne displays the primary domain with a red underscore.



Moving a Domain

You cannot use ConsoleOne to move a Domain object to a different location in the eDirectory tree because it is a container object. Only leaf objects can be moved. If you need to change the context, graft the GroupWise domain to its corresponding eDirectory object in the new container location. See "GW / eDirectory Association" on page 73 for more information about grafting objects.

You can, however, move the domain directory and the domain database (wpdomain.db) by copying the domain directory structure and all its contents to the new location.

IMPORTANT: Follow these instructions if you want to move a domain on a NetWare or Windows server to another directory on the same server or to a different NetWare or Windows server. If you want to move a domain located on a NetWare or Windows server onto a Linux server, see "Moving a Domain to Linux" in "Update" in the *GroupWise 6.5 Installation Guide*.

1 Back up the domain. See Chapter 31, "Backing Up GroupWise Databases," on page 375.

2 In ConsoleOne, browse to and right-click the domain to move, then click Properties to display the domain Identification page.

3 In the UNC Path field, change the UNC path to the location where you want to move the domain, then click OK to save the new location.

   The location change will be propagated throughout your GroupWise system.

4 Stop the MTA and any gateways running for the domain.

5 Use `xcopy` with the `/s` and `/e` options to copy the domain directory and database to the new location. These options re-create the same directory structure even if directories are empty.

   Example: `xcopy` *`domain_directory`* `/s /e` *`destination`*

6 Give rights to all objects that need to access the domain database.

   For example, the NetWare® MTA needs rights if the new location is on a different server.

7 Edit the MTA and gateway startup files to reflect the changes, then restart the MTA and gateways.

   See "Adjusting the MTA for a New Location of a Domain or Post Office" on page 587.

8 When you are sure the domain is functioning properly in its new location, delete the original domain directory and its contents.

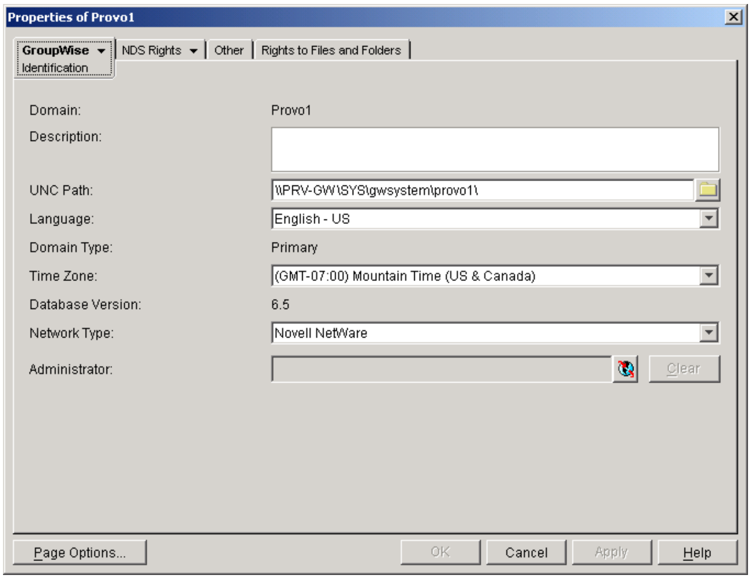
If you need to move the MTA along with its domain, see "Moving the MTA to a Different Server" on page 586.

Deleting a Domain

You can delete a domain only when it no longer owns subordinate GroupWise objects. For example, you cannot delete the primary domain of your GroupWise system if it still owns secondary domains.You cannot delete a secondary domain if it still owns post offices. However, MTA and Gateway objects are automatically deleted along with the Domain object.

1 In ConsoleOne, connect to the primary domain of your GroupWise system, as described in "Connecting to a Domain" on page 123.

2 Browse to and right-click the Domain object you want to delete, then click Properties to display the domain Identification page.


Properties of Provo1

Domain: Provo1

Description:

UNC Path: \\PRV-GW\SYS\gwsystem\provo1\

Language: English - US

Domain Type: Primary

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

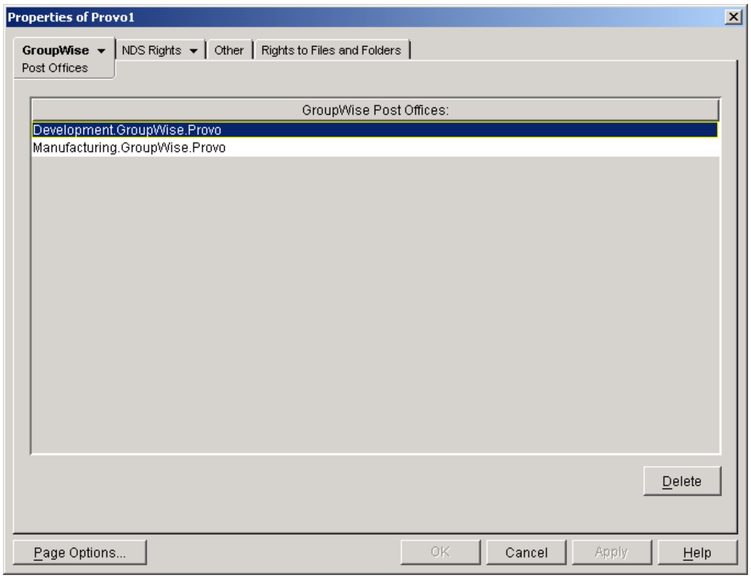
Database Version: 6.5

Network Type: Novell NetWare

Administrator:

3 Verify that the current directory path displayed on the domain Identification page is correct.

4 Click Post Offices, then move or delete any post offices that belong to this domain. See "Moving a Post Office" on page 183 and "Deleting a Post Office" on page 184.


Properties of Provo1

GroupWise Post Offices:

Development.GroupWise.Provo
Manufacturing.GroupWise.Provo

5 Right-click the Domain object, then click Delete to delete the Domain object from eDirectory.

6 When prompted, click Yes to delete the corresponding domain directory structure.

7 Stop the MTA for the domain and uninstall the MTA software if applicable.

See "Stopping the MTA" on page 609 and "Uninstalling the MTA Software" on page 573.

Changing MTA Configuration to Meet Domain Needs

Because the MTA transfers messages between domains and between post offices in the same domain, its functioning affects the domain itself, local users in post offices belonging to the domain, and users who exchanges messages with local users in the domain. Proper MTA configuration is essential for a smoothly running GroupWise system. Complete details about the MTA are provided in "Message Transfer Agent" on page 555. As you create and manage domains, you should keep in mind the following aspects of MTA configuration:

- "Enhancing Domain Security with SSL Connections to the MTA" on page 589
- "Restricting Message Size between Domains" on page 588
- "Scheduling Direct Domain Links" on page 593
- "Optimizing TCP/IP Links" on page 635

10 Managing the Links between Domains and Post Offices

When you create a new secondary domain in your GroupWise® system or a new post office in a domain, you configure one direct link to connect the new domain or post office to a domain in your GroupWise system. For simple configurations, this initial link might be adequate. For more complex configurations, you must modify link types and protocols to achieve optimum message flow throughout your GroupWise system.

The following topics help you manage links between domains and post offices:

- "Understanding Link Configuration" on page 131
- "Using the Link Configuration Tool" on page 136
- "Interpreting Link Symbols" on page 143
- "Modifying Links" on page 144

Understanding Link Configuration

In GroupWise, a link is defined as the information required to route messages between domains, post offices, and gateways in a GroupWise system. Initial links are created when domains, post offices, and gateways are created. The following topics help you understand link configuration:

- "Domain-to-Domain Links" on page 131
- "Domain-to-Post Office Links" on page 134
- "Link Protocols for Direct Links" on page 134

Domain-to-Domain Links

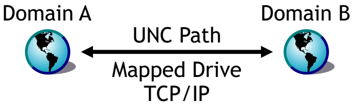
The primary role of the MTA is to route messages from one domain to another. Domain links tell the MTA how to route messages between domains. Domain links are stored in the domain database (wpdomain.db). There are three types of links between source and destination domains:

- "Direct Links" on page 132
- "Indirect Links" on page 132
- "Gateway Links" on page 134

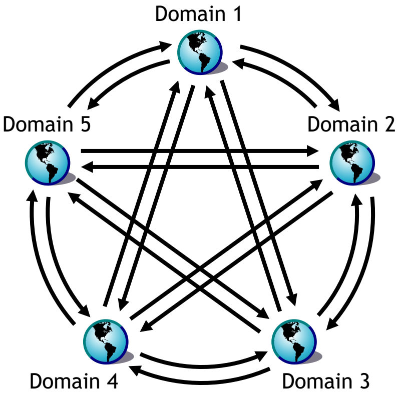
As an alternative to configuring individual links between individual domains throughout your GroupWise system, you can establish a system of one or more routing domains. See "Using Routing Domains" on page 591.

Direct Links

In a direct link between domains, the source domain's MTA communicates directly with the destination domain's MTA. If it is using a TCP/IP link, the source domain MTA communicates messages to the destination domain MTA by way of TCP/IP, which does not require disk access by the source MTA in the destination domain. If it is using a mapped or UNC link, the source domain MTA writes message files into the destination domain MTA input queue, which does require disk access by the source MTA in the destination domain. For additional details about the configuration options for direct links, see "Link Protocols for Direct Links" on page 134.



Direct links can be used between all domains. This is a very efficient configuration but might not be practical in a large system.



Indirect Links

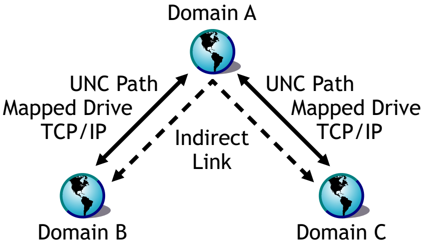
In an indirect link between domains, the source domain's MTA routes messages through one or more intermediate MTAs in other domains to reach the destination domain's MTA. In other words, an indirect link is a series of two or more direct links. In large systems, direct links between each pair of domains might be impractical, so indirect links can be common. A variety of indirect link configurations are possible, including:

- "Simple Indirect Links" on page 133
- "Star Configuration" on page 133
- "Two-Way Ring Configuration" on page 133
- "Combination Configuration" on page 134

Properly configured links optimize message flow throughout your GroupWise system.

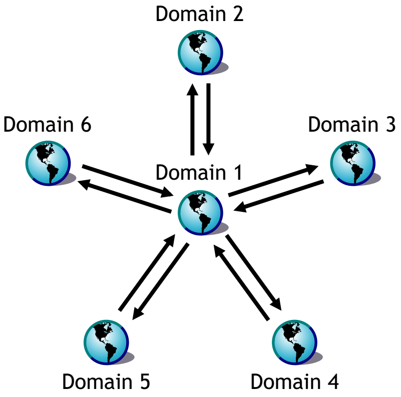
Simple Indirect Links

In simplest form, an indirect link can be used to pass messages between two domains that are not directly linked.



Star Configuration

In a star configuration, one central domain is linked directly to all other domains in the system. All other domains are indirectly linked to each other through the central domain.

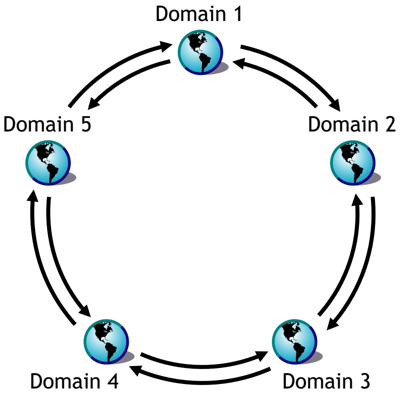


If you have more than ten domains, you might want to designate the central domain as a routing domain. The sole function of a routing domain is to transfer messages between other domains; it has no post offices of its own. See "Using Routing Domains" on page 591.

The major drawback of the star configuration is that the central domain is a single point of failure.

Two-Way Ring Configuration

In a two-way ring configuration, each domain is directly linked to the next and previous domains in the ring and indirectly linked to all other domains in the system.



An advantage of the two-way ring configuration is that it has no single point of failure. A disadvantage is that, depending on the size of the system, a message might go through several domains before arriving at its destination. A two-way ring works well in a system with five domains or less because transferring a message never requires more than two hops.

Combination Configuration

These three basic link configurations can be combined in any way to meet the needs of your GroupWise system.

Gateway Links

In a gateway link between domains, the sending domain's MTA must route the message through a gateway to reach its destination. Gateways can be used to:

- Link domains within your GroupWise system. See "Using Gateway Links between Domains" on page 583.
- Link your GroupWise system to another GroupWise system through an external domain. See "Using Direct Links" in "Connecting to GroupWise 5.x and 6.x Systems" in the *GroupWise 6.5 Multi-System Administration Guide*
- Link your GroupWise system to a different e-mail system through a non-GroupWise domain. See "Connecting to Non-GroupWise Messaging Systems" in the *GroupWise 6.5 Multi-System Administration Guide*.

A variety of GroupWise gateways are available. For a list of gateways, see GroupWise 6.*x* Gateways (http://www.novell.com/documentation/gw6xgate/index.html). GroupWise 5.5 gateways can be used with GroupWise 6.*x*.

You cannot locate a post office across a gateway link from its domain. This would preclude locating a post office across a modem connection.

Domain-to-Post Office Links

Between a domain and its post offices, all links must be direct links. There are no alternative link types between a domain and its post offices.

Link Protocols for Direct Links

The link protocol of a direct link between domains determines how the MTAs for the domains communicate with each other across the link. When you create a new domain, you must link it to an existing domain. This creates the initial domain-to-domain link.

Between a domain and a post office, the link protocol determines how the MTA transfers messages to the post office. Messages do not flow directly from one post office to another within a domain. Instead, they are routed through the domain. When you create a new post office, you must specify which domain it belongs to. This creates the initial domain-to-post office link.

There are three link protocols for direct links between domains and between a domain and its post offices:

- "TCP/IP Links" on page 135
- "Mapped Links" on page 135
- "UNC Links" on page 135

NOTE: On Linux, TCP/IP links are required.

TCP/IP Links

Domain-to-Domain TCP/IP Links

In a TCP/IP link between domains, the source MTA and the destination MTA communicate by way of TCP/IP rather than by writing message files. The source MTA establishes a TCP/IP link with the destination MTA and transmits whatever messages need to go to that domain. The destination MTA receives the messages and routes them on to local post offices or to other domains as needed. During the process, message files are created in the gwinprog directory for backup purposes and are deleted when the TCP/IP communication process is completed.

Domain-to-Post Office TCP/IP Links

In a TCP/IP link between a domain and a post office, you must configure both the POA and the MTA for TCP/IP. The source MTA establishes a TCP/IP link with the destination POA and transmits whatever messages need to go to that post office. The destination POA receives the messages and delivers them into mailboxes in the post office. During this process, message files are created in the POA input queue for backup purposes and are deleted when delivery is completed.

Mapped Links

Domain-to-Domain Mapped Links

In a mapped link between domains, the location of the destination domain is specified in the following format:

`drive:\domain_directory`

The source MTA writes message files into its output queue at the location:

`drive:\domain_directory\wpcsin`

as input for the destination domain's MTA. Because drive mappings are changeable, you could move the domain directory structure, map its new location to the original drive letter, and the domain-to-domain link would still be intact.

Domain-to-Post Office Mapped Links

In a mapped link between a domain and a post office, the location of the post office is specified in the following format:

`drive:\post_office_directory`

The MTA writes message files into its output queue at the location:

`drive:\post_office_directory\wpcsout`

as input for the post office's POA. Because drive mappings are changeable, you could move the post office directory structure, map its new location to the original drive letter, and the domain-to-post office link would still be intact.

UNC Links

Domain-to-Domain UNC Links

In a UNC link between domains, the location of the destination domain is specified in the following format:

\\server\volume\domain_directory

The source MTA writes message files into its output queue at the location:

\\server\volume\domain_directory\wpcsin

as input for the destination domain's MTA. Because UNC paths represent absolute locations on your network, if you move the domain to a new location, you would need to edit the link to match.

Domain-to-Post Office UNC Links

In a UNC link between a domain and a post office, the location of the post office is specified in the following format:

\\server\volume\post_office_directory

The MTA writes message files into its output queue at the location:

\\server\volume\post_office_directory\wpcsout

as input for the post office's POA. Because UNC paths represent absolute locations in your network, if you move the post office to a new location, you would need to edit the link to match.

Using the Link Configuration Tool

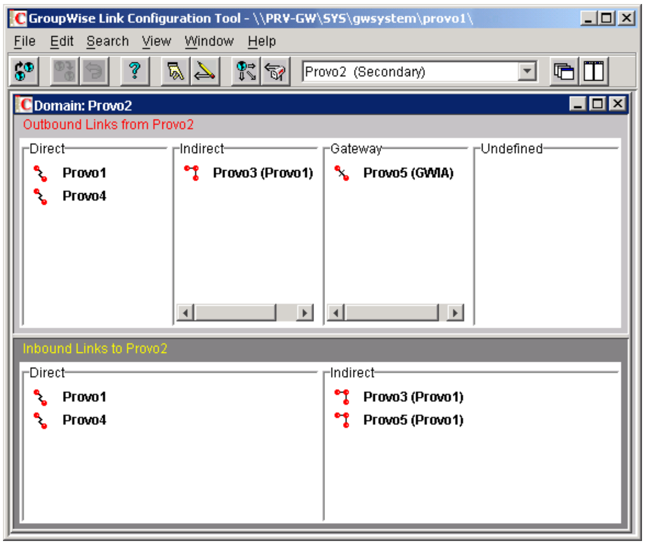
The Link Configuration tool helps you manage the links between the domains and post offices in your GroupWise system. The following topics help you perform basic link management tasks:

- "Starting the Link Configuration Tool" on page 136
- "Editing a Domain Link" on page 138
- "Editing Multiple Domain Links" on page 139
- "Editing a Post Office Link" on page 140
- "Viewing the Path of an Indirect Link between Domains" on page 141
- "Viewing the Indirect Links Passing through a Domain" on page 141
- "Viewing the Gateway Links Passing through a Gateway" on page 142
- "Saving and Synchronizing Link Configuration Information" on page 143

Starting the Link Configuration Tool

The Link Configuration tool is provided to help you change from default links to whatever link configuration best suits your GroupWise system.

1. In ConsoleOne®, select the Domain object whose links you want to modify.
2. Click Tools > GroupWise Utilities > Link Configuration to display the Link Configuration Tool window.


GroupWise Link Configuration Tool - \\PRV-GW\SYS\gwsystem\provo1\
File
Edit
Search
View
Window
Help
Provo2 (Secondary)

Domain: Provo2

Outbound Links from Provo2

Direct	Indirect	Gateway	Undefined
Provo1	Provo3 (Provo1)	Provo5 (GWIA)	
Provo4			

Inbound Links to Provo2

Direct	Indirect
Provo1	Provo3 (Provo1)
Provo4	Provo5 (Provo1)

The most frequently used features of the Link Configuration tool are available on the toolbar:

Button	Menu Equivalent	Function
	File > Open	Open a different domain database (wpdomain.db) to modify links in a different domain
	File > Save	Save the current link configuration information to the domain database
	Edit > Undo	Undo your changes to the link configuration (since the last save)
?	Help > Help	Display online Help for the Link Configuration tool
	Search > Find	Search for a specified domain
	Double-click object	Display details of the selected object
	View > Domain Links	View domain links for the selected domain
	View > Post Office Links	View post office links for the selected domain

3 Continue with a specific link management task:

- "Editing a Domain Link" on page 138
- "Editing Multiple Domain Links" on page 139
- "Editing a Post Office Link" on page 140
- "Viewing the Path of an Indirect Link between Domains" on page 141
- "Viewing the Indirect Links Passing through a Domain" on page 141
- "Viewing the Gateway Links Passing through a Gateway" on page 142

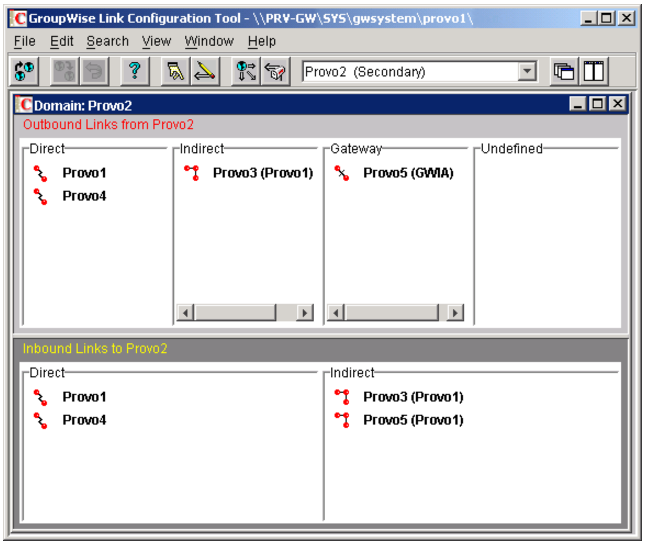
Editing a Domain Link

After starting the Link Configuration tool:

1 From the drop-down list, select the domain whose links you want to edit.

2 Click View > Domain Links to display domain links.

Outbound and inbound links for the selected domain are listed.



GroupWise Link Configuration Tool - \\PRV-GW\SYS\gwsystem\provo1\

Provo2 (Secondary)

Domain: Provo2

Outbound Links from Provo2

Direct: Provo1, Provo4

Indirect: Provo3 (Provo1)

Gateway: Provo5 (GWIA)

Undefined

Inbound Links to Provo2

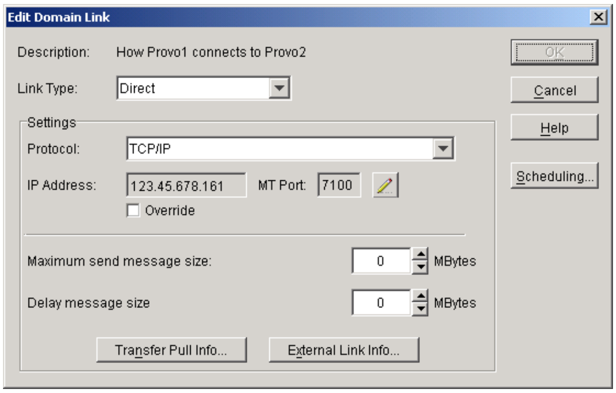
Direct: Provo1, Provo4

Indirect: Provo3 (Provo1), Provo5 (Provo1)

3 Double-click a domain in the Outbound Links list to edit the link to that domain from the selected domain.

or

Double-click a domain in the Inbound Links list to edit the link from that domain to the selected domain.



Edit Domain Link

Description: How Provo1 connects to Provo2

Link Type: Direct

Settings

Protocol: TCP/IP

IP Address: 123.45.678.161 MT Port: 7100

□ Override

Maximum send message size: 0 MBytes

Delay message size 0 MBytes

TIP: You can also open the Edit Domain Link dialog box by dragging a domain from one link type to another.

4 Select the link type.

- "Direct Links" on page 132
- "Indirect Links" on page 132
- "Gateway Links" on page 134

5. For a direct link, select the link protocol.
   - "Mapped Links" on page 135
   - "UNC Links" on page 135
   - "TCP/IP Links" on page 135
6. Provide the location of the domain in the format appropriate to the selected protocol.
7. Click OK.
8. Repeat Step 1 through Step 7 for whatever links you need to modify.

   As a time-saving measure, you can make a new domain's links the same as an existing domain's links. Click Edit > Default Links, then click the domain whose links you want to use as a pattern for the new domain. Select Outbound and/or Inbound as needed, then click OK.

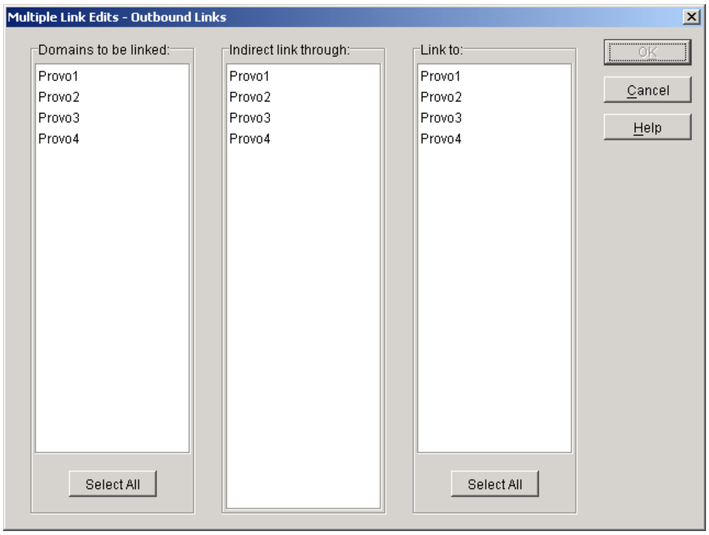
   To look at the same link information from different points of view, you can start the Link Configuration tool multiple times to open multiple Link Configuration Tool windows.
9. To exit the Link Configuration Tool and save your changes, click File > Exit > Yes.

Editing Multiple Domain Links

When your GroupWise system includes indirect links, it is not unusual for several domains to link to the same domain. As a time-saving measure, you can create links from multiple domains to the same domain in one operation.

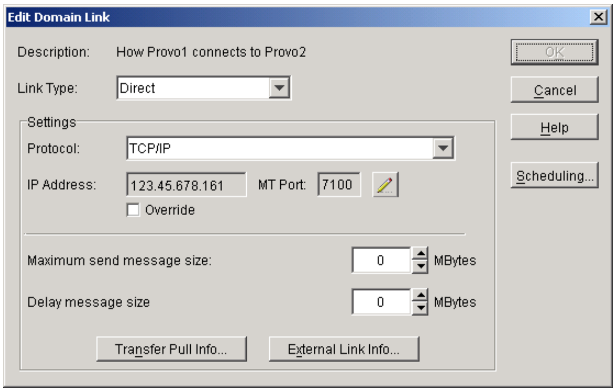
After starting the Link Configuration tool:

1. Click Edit > Multiple Link Edits.



2. In the Domains to Be Linked column, select the source domains whose outgoing links you want to modify.
3. In the Indirect Link Through column, select the intermediate domain through which you want the indirect links to pass.
4. In the Link To column, select one or more destination domains.
5. Click OK.

6 Fill in the fields in the Edit Domain Link dialog box for each direct link between a source domain and the intermediate domain, as described in "Editing a Domain Link" on page 138, then click OK.



Edit Domain Link

Description: How Provo1 connects to Provo2

Link Type: Direct

Settings

Protocol: TCP/IP

IP Address: 123.45.678.161 MT Port: 7100

□ Override

Maximum send message size: 0 MBytes

Delay message size 0 MBytes

The Edit Domain Link dialog box continues to appear until you have defined all the direct links between the source domains and the intermediate domain.

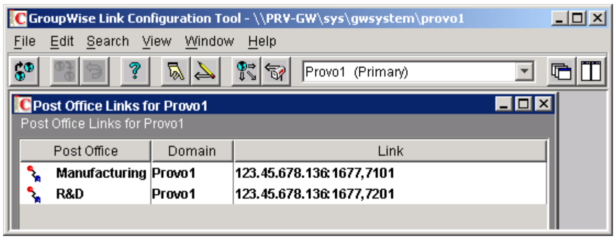
IMPORTANT: After defining links from the source domains to the intermediate domain, make sure the links from the intermediate domain to other domains are set up correctly.

Editing a Post Office Link

After starting the Link Configuration tool:

1 From the drop-down list, select the domain whose post office link you want to edit.

2 Click View > Post Office Links to display post office links.



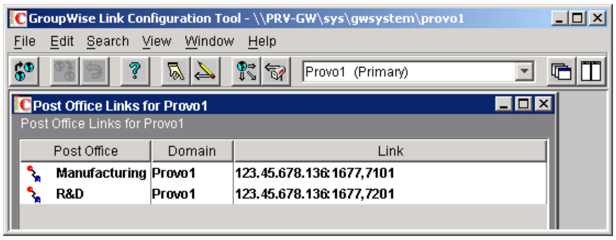
GroupWise Link Configuration Tool - \\PRV-GW\sys\gwsystem\provo1

Post Office Links for Provo1

Post Office Links for Provo1

Post Office	Domain	Link
Manufacturing	Provo1	123.45.678.136:1677,7101
R&D	Provo1	123.45.678.136:1677,7201

3 Double-click a post office to edit the link from the domain to the post office.



GroupWise Link Configuration Tool - \\PRV-GW\sys\gwsystem\provo1

Post Office Links for Provo1

Post Office Links for Provo1

Post Office	Domain	Link
Manufacturing	Provo1	123.45.678.136:1677,7101
R&D	Provo1	123.45.678.136:1677,7201

4 Select the link protocol for the direct link.

- "Mapped Links" on page 135
- "UNC Links" on page 135
- "TCP/IP Links" on page 135

5 Provide the location of the post office in the format appropriate to the selected protocol.

6 For a TCP/IP link, provide the message transfer port number where you want the POA to listen for incoming messages from the MTA.

The default message transfer port for the POA is 7101.

7 Click OK.

8 To exit the Link Configuration tool and save your changes, click File > Exit > Yes.

Viewing the Path of an Indirect Link between Domains

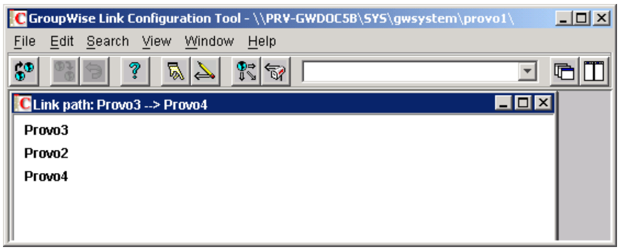
The more hops between two indirectly linked domains, the longer it takes a message to travel between them. To make sure the number of hops between two indirectly linked domains is as small as possible, you can list the route a message would take from one domain to the other in ConsoleOne.

After starting the Link Configuration tool:

1 Select a domain from the drop-down list.

2 Select a domain in the Indirect links list.

3 Click View > Link Path to see a list of the hops between the two domains.



GroupWise Link Configuration Tool - \\PRV-GWDOC5B\SYS\gwsystem\provo1\

Link path: Provo3 --> Provo4

Provo3
Provo2
Provo4

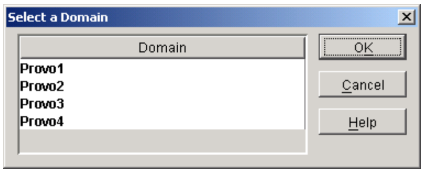
You can also use GroupWise Monitor to trace the path a message would take between two domains. See “Link Trace Report” on page 931 and “Tracing a Link at the Monitor Web Console” on page 950.

Viewing the Indirect Links Passing through a Domain

If a domain serves as a hop in an indirect link, making changes to that domain could affect all indirect links passing through that domain. You can list all the indirect links that pass through a domain in ConsoleOne.

After starting the Link Configuration tool:

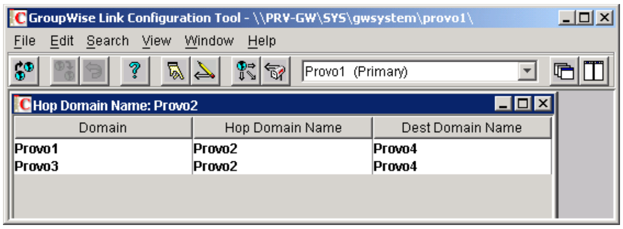
1 Click View > Link Hop to list all domains in your system.



Select a Domain

Domain
Provo1
Provo2
Provo3
Provo4

2 Double-click a domain to list the indirect links passing through it.



Domain	Hop Domain Name	Dest Domain Name
Provo1	Provo2	Provo4
Provo3	Provo2	Provo4

3. If you need to reroute a link, right-click the link, then click Edit to open the Edit Domain Link dialog box and make changes as needed.

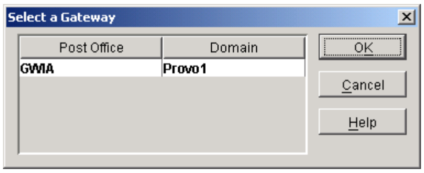
You can also use GroupWise Monitor to check the links passing through a selected domain. See "Link Configuration Report" on page 932 and "Checking Links Configuration at the Monitor Web Console" on page 950. However, you cannot change link information using Monitor.

Viewing the Gateway Links Passing through a Gateway

Before making changes to a gateway, you can list all the links that pass through the gateway.

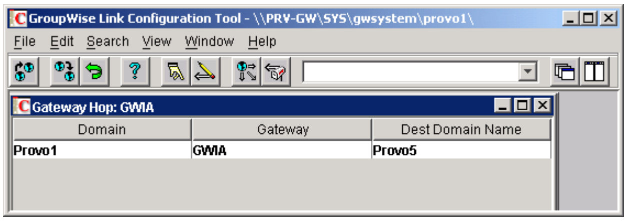
After starting the Link Configuration tool:

1. Click View > Gateway Hop to list all gateways in your system.



Post Office	Domain
GWIA	Provo1

2. Double-click a gateway to list the domains linked through that gateway.


GroupWise Link Configuration Tool - \\PRV-GW\SYS\gwsystem\provo1\
File
Edit
Search
View
Window
Help
Gateway Hop: GWIA

Domain	Gateway	Dest Domain Name
Provo1	GWIA	Provo5

3. If you need to reroute a link, right-click the link, then Edit to open the Edit Domain Link dialog box and make changes as needed.

Saving and Synchronizing Link Configuration Information

Whenever you modify link configuration information, a cautionary symbol (see “Link Status Symbols” on page 143) appears next to the modified link until you save the current link configuration by clicking Edit > Save. If you are making extensive changes to link configuration information, you should save regularly. When you save, the information is written out to the domain database (wpdomain.db) for the domain to which you are currently connected. You can change to a different domain database without exiting the Link Configuration tool by clicking File > Open.

The MTA routinely synchronizes the information in the domain databases throughout your GroupWise system. If you are making extensive changes to link configuration information, you can synchronize the information immediately by clicking Edit > Synchronize.

Interpreting Link Symbols

As you modify links, you see symbols that represent the various link types. Along with the link type symbols, you sometimes see link status symbols.

- “Link Type Symbols” on page 143
- “Link Status Symbols” on page 143

Link Type Symbols

Link Type Symbol	Meaning
	Direct link
	Indirect link
	Gateway link
	TCP/IP link to domain
	TCP/IP link to post office
	Undefined link

Link Status Symbols

Link Status Symbol	Meaning
	Link modification not yet saved
	Link modification not yet synchronized
	Insufficient rights to modify link
	Rights not yet checked

Modifying Links

In “Post Office Agent” on page 415 and “Message Transfer Agent” on page 555, detailed instructions for changing link types are provided as outlined below:

Changing the Link Protocol between the Post Office and the Domain

- “Using TCP/IP Links between the Post Office and the Domain” on page 443
- “Using Mapped or UNC Links between the Post Office and the Domain” on page 444

Changing the Link Protocol between Domains

- “Using TCP/IP Links between Domains” on page 579
- “Using Mapped or UNC Links between Domains” on page 582
- “Using Gateway Links between Domains” on page 583

Customizing Link Configuration

- “Using Routing Domains” on page 591
- “Scheduling Direct Domain Links” on page 593
- “Using a Transfer Pull Configuration” on page 596

III Post Offices

11 Creating a New Post Office

As your GroupWise® system grows, you typically need to add new post offices.

- "Understanding the Purpose of Post Offices" on page 147
- "Planning a New Post Office" on page 148
- "Setting Up the New Post Office" on page 158
- "What's Next" on page 162

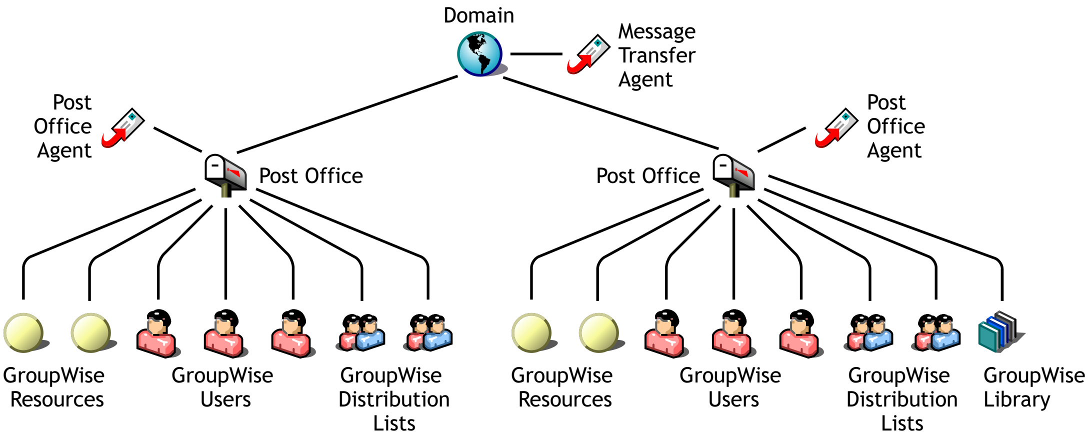
IMPORTANT: If you are creating a new post office in a clustered GroupWise system, see the appropriate section of the GroupWise 6.5 Interoperability Guide before you create the post office:

- "Setting Up a Domain and Post Office in a Novell Cluster" in "Novell Cluster Services"
- "Setting Up a Domain and Post Office in a Microsoft Cluster" in "Microsoft Clustering Services"

Understanding the Purpose of Post Offices

The post office serves as an administrative unit for a group of users and is used for addressing messages. Each GroupWise user has an address that consists of a user ID, the user's post office name, the GroupWise domain name, and, optionally, an Internet domain name.

The following diagram illustrates the logical organization of a GroupWise domain with multiple post offices. The two post offices belong to the domain. All of the objects under each post office belong to that post office.



As illustrated above, each post office must have at least one Post Office Agent (POA) running for it. The POA delivers messages to users' mailboxes and performs a variety of post office and mailbox maintenance activities.

When you add a new post office, you must link it to a domain. The link defines how messages travel between the post office and its domain. Links are discussed in detail in Chapter 10, “Managing the Links between Domains and Post Offices,” on page 131.

Physically, a post office consists of a set of directories that house all the information stored in the post office. To view the structure of the post office directory, see “Post Office Directory” in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. The post office directory contains users’ mailboxes and messages, as well as other vital information. For an overview, see “Information Stored in the Post Office” on page 418.

Planning a New Post Office

This section provides the information you need in order to decide when, where, and how to create a new post office. The “Post Office Worksheet” on page 163 lists all the information you need as you set up your post office. You should print the worksheet and fill it out as you complete the tasks listed below.

- “Determining When to Add a Post Office” on page 148
- “Selecting the Domain That the Post Office Will Belong To” on page 149
- “Determining the Context for the Post Office Object” on page 150
- “Choosing the Post Office Name” on page 151
- “Deciding Where to Create the Post Office Directory” on page 152
- “Deciding Where to Install the Agent Software” on page 153
- “Deciding How to Link the New Post Office” on page 156
- “Selecting the Post Office Language” on page 156
- “Selecting the Post Office Time Zone” on page 156
- “Selecting a Software Distribution Directory” on page 156
- “Selecting a Post Office Security Level” on page 157
- “Deciding if You Want to Create a Library for the New Post Office” on page 157

After you have completed the tasks and filled out the “Post Office Worksheet” on page 163, you are ready to continue with “Setting Up the New Post Office” on page 158.

Determining When to Add a Post Office

After you have your basic GroupWise system up and running, you might need to expand it. How do you know when you should add a post office? The answer to this depends on your company organization, the number of users on your network, and the physical limitations of your network servers.

- “Physical Organization” on page 149
- “Logical Organization” on page 149
- “Number of Users” on page 149
- “Demand on the POA” on page 149

Physical Organization

If your network spans several sites, you might want to create post offices (if not domains) at each physical location. This reduces the demands on long distance network links.

Logical Organization

Processing messages within a post office is faster and typically generates less network traffic than messages traveling between different post offices. As you expand GroupWise, you might find it useful to add post offices in order to group users who frequently send mail to each other.

Grouping users into post offices, based upon company organization or job function, makes administrative tasks, such as creating distribution lists, limiting Address Book visibility, and distributing shared folders, easier. For example, some employees might work in corporate functions like accounting and human resources. Other employees might be involved in sales and marketing and frequently attend meetings together, requiring frequent busy searches. Some areas, for example the production floor, might not need a workstation or user account for each individual.

Number of Users

Although a GroupWise post office can support more than 10,000 users, you should consider adding a post office when an existing post office has more than about 1000 to 2500 users and you expect it to keep growing. There are several reasons for this:

- It minimizes the impact if you have a problem with a server.
- It keeps the time required to perform post office and mailbox maintenance activities including backups from becoming excessive.
- It allows room to grow while maintaining best performance.

Therefore, a good post office size is about 1000 to 2500 users and include all of the resources (such as equipment, company cars, and conference rooms) and distribution lists they might need.

Demand on the POA

The POA is a very flexible component of your GroupWise system. Many aspects of its functioning are configurable, to meet the particular needs of the post office it services, no matter what the size. In addition, you can choose to run multiple POAs for the same post office, in order to specialize its functioning, as described in:

- "Configuring a Dedicated Client/Server POA" on page 510
- "Configuring a Dedicated Message File Processing POA" on page 513
- "Configuring a Dedicated Indexing POA" on page 516
- "Configuring a Dedicated Database Maintenance POA" on page 518

As a result, the choice is up to you whether you prefer a single, large post office, perhaps with multiple POAs, or multiple smaller post offices, each with its own POA.

Selecting the Domain That the Post Office Will Belong To

A post office is associated with a specific domain, even though it might reside in a different organizational unit in the Novell® eDirectory™ tree. If you have just one domain, the new post office will belong to it. If you want to create a new domain as well as a new post office, see Chapter 8, "Creating a New Domain," on page 109.

In a multiple post office system, the domain organizes post offices into a logical grouping for addressing and routing purposes. Each user in the domain has a GroupWise address that consists of the user's GroupWise ID, the post office name, the GroupWise domain name, and optionally, an Internet domain name.

Domains function as the main administration units for the GroupWise system. Post office information is stored in the domain database, as well as in the post office database. Changes are distributed to each post office database from the domain.

WORKSHEET
Under Item 3: GroupWise Domain, specify the GroupWise domain that the new post office will belong to.

The items in the worksheet are listed in the order you enter them when setting up your post office. This planning section does not follow the same order as the worksheet, but all worksheet items are covered.

Determining the Context for the Post Office Object

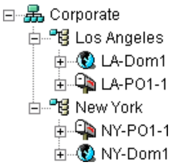
The eDirectory context of the Post Office object determines how you administer the post office. The post office can be created in any organization or organizational unit as long as it is in the same tree as the domain. The following diagrams provide some examples of how domains can be placed in the eDirectory tree:

- "GroupWise Objects Reflect Physical Locations" on page 150
- "GroupWise Objects Reflect Company Organization" on page 151
- "GroupWise Objects Are Grouped with Servers" on page 151
- "GroupWise Objects Are Located in a Separate GroupWise Container" on page 151

WORKSHEET
Under Item 1: eDirectory Container, specify the name of the eDirectory container where you want to create the new post office.

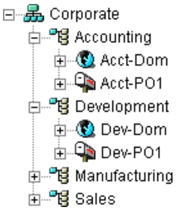
GroupWise Objects Reflect Physical Locations

The GroupWise system below focuses on the physical layout of the company. Because most mail traffic is generated by users in the same location, the mail traffic across the WAN is minimized. An organizational unit was created for each site. A domain and post office were created under each organizational unit, corresponding to the city. The sites can be administered centrally or at each site. Administrator rights can be assigned at the domain level.



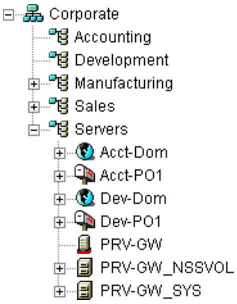
GroupWise Objects Reflect Company Organization

The following GroupWise system focuses on departmental organization, as does the eDirectory tree. GroupWise domains and post offices parallel eDirectory organizational units, placing the domains and post offices within the organizational units containing the users that belong to them.



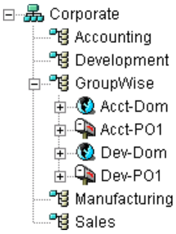
GroupWise Objects Are Grouped with Servers

Because domains and post offices have directory structures on network servers, you could also choose to place the Domain and Post Office objects in the same context as the servers where the directories reside, as shown in the following example.



GroupWise Objects Are Located in a Separate GroupWise Container

Domains and post offices can also be created in their own organizational unit. Administratively, this approach makes it easier to restrict a GroupWise administrator’s object and property rights to GroupWise objects only.



Choosing the Post Office Name

The post office must be given a unique name. The name is used for addressing and routing purposes within GroupWise, and might appear in the GroupWise Address Book.

The post office name can reflect a location, organization, department, and so on. For example, you might want the domain name to be the location (for example, Provo) while the post office name is one of the company’s departments (for example, Research). Name the new post office carefully. After it is created, the name cannot be changed.

The post office name can consist of one or more words. Use underscores (_) rather than spaces as separators between words to facilitate addressing across the Internet. Do not use any of the following invalid characters in the post office name:

ASCII characters 0-13

Asterisk *

At sign @

Braces { }

Colon :

Comma ,

Double quote "

Extended characters

Parentheses ( )

Period .

WORKSHEET

Under Item 2: Post Office Name, specify the post office name.

Under Item 9: Post Office Description, provide a description for the post office to help you identify its function in the system.

Deciding Where to Create the Post Office Directory

Logically, the Post Office object resides in eDirectory and is administered through ConsoleOne®. Physically, the post office has a directory structure for databases, message queues, and other files. The post office directory structure can be created on NetWare® servers (NetWare 6.*x*, NetWare 5.*x*, NetWare 4.2, or NetWare 3.12), Linux servers (SUSE Standard or Enterprise Server 8, Red Hat* Enterprise Linux 3 ES or AS), or Windows servers (Windows 2000 or Windows NT). The server where you create the post office directory structure can be in the same tree as the Post Office object or in another tree.

Databases and directories in the post office are updated as messages are sent. Because the POA typically makes these updates, we recommend that you place the post office directory on a server that can be easily accessed by the POA and, depending on configuration, the MTA. Users typically need a TCP/IP connection to the POA in order to access their mailboxes.

When you are planning the post office directory location and which users will belong to the post office, consider the following:

- **Post Office Directory Space Requirements:** You need a minimum of 50 MB for each user. Because the message store can require considerable disk space, we recommend you allow each user at least 200 MB of storage space. You should also take into consideration the size of attachments, and your archive and delete policies. If message attachments are large and you are not planning to require users to archive or delete old messages, allow more storage. If you are creating libraries you need even more, depending on the size and number of documents. For details about managing post office disk space, see "Managing Disk Space Usage in the Post Office" on page 171.
- **Network Access by the POA:** The POA must have direct network access (mapped drive or file system mount) to the post office directory. This issue is discussed in detail in "Deciding Where to Install the Agent Software" on page 153.
- **Security from User Access:** Users typically access their mailboxes through a TCP/IP connection to the POA. Therefore, users do not need access to the post office directory. You should create it in a location you can easily secure; otherwise, you could have files inadvertently moved or deleted.

Choose an empty directory for the new post office. If you want, the directory can reflect the name of the post office, for example research for the Research post office. On NetWare, use a maximum of 8 characters in the directory name. On Linux, use only lowercase characters in the directory name.

Choose the name and path carefully. After the post office directory is created, it is difficult to rename it. If the directory you specify does not exist, it is created when you create the post office. Do not create the post office directory under another domain or post office directory.

WORKSHEET

Under Item 4: Post Office Database Location, specify the full path for the post office directory.

Under Item 10: Network Type, record the network type in use at that location.

Deciding Where to Install the Agent Software

You must run a new instance of the POA for each new post office. To review the functions of the POA for the post office, see "Role of the Post Office Agent" on page 423. For complete installation instructions and system requirements, see "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

When planning the installation of the POA, you need to consider how the new post office links to its domain. For an overview of link configuration, see Chapter 10, "Managing the Links between Domains and Post Offices," on page 131.

The POA requires direct network access (mapped drive or file system mount) to the post office directory. Consider the following alternatives when selecting a location for the POA:

- "POA Access to the New Post Office: Local vs. Remote" on page 153
- "MTA Access to the New Post Office: Mapped and UNC Links vs. TCP/IP Links" on page 154
- "Cross-Platform Issues" on page 155

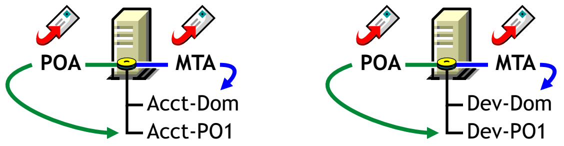
WORKSHEET

Under Item 12: Agent Location, indicate whether you plan to run the POA on the same server where the post office directory is located, or on a different server.

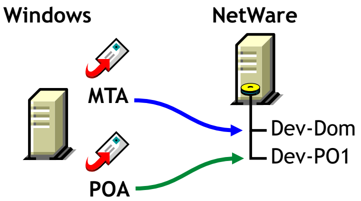
Under Item 13: Agent Platform, specify the platform where the POA will run (NetWare, Linux, or Windows).

POA Access to the New Post Office: Local vs. Remote

Running the POA locally on the same server where the post office resides simplifies network connections (no login is required), reduces network traffic, and protects database integrity. In the following diagram, the agent software is installed on the same server where the domain and post office reside.



Running the POA on a remote server allows you to place the heaviest processing load on your highest performing server. In the following diagram, the agent software is installed on a different server from where the domains and post offices reside.

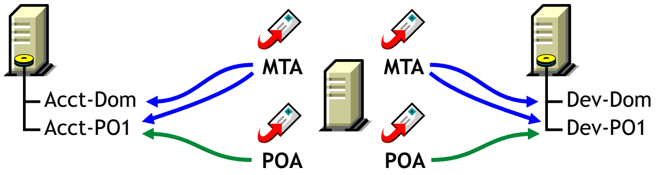


When you run the POA on a different server from where its directory structure and databases are located, you need to provide adequate access.

- If the NetWare® POA needs direct network access to another NetWare server where the post office is located, you must add the /dn switch or the /user and /password switches to the POA startup file to provide authentication information. Username and password information can also be provided in the Remote File Server Settings box of the Post Office Settings page in ConsoleOne.
- If the Linux POA needs direct network access to another Linux server, you must mount the file system where the post office is located before you start the Linux POA.
- If the Windows POA needs direct network access to another Windows server where the post office is located, you must map a drive to the other server before you start the Windows POA.

MTA Access to the New Post Office: Mapped and UNC Links vs. TCP/IP Links

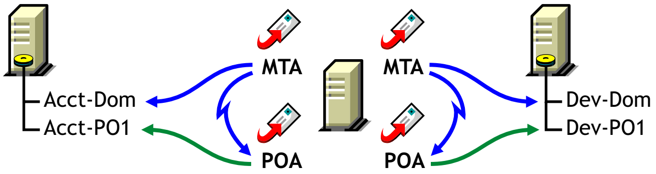
If a domain includes multiple post offices, the new post office will probably reside on different server from where the domain is located. If you plan to use mapped or UNC links between the domain and the new post office, the MTA requires the same access to the post office directory as it requires to the domain directory.



- If the NetWare MTA needs direct network access to a new post office on another NetWare server, you must add the /dn switch or the /user and /password switches to the MTA startup file to provide authentication information.
- If the Windows MTA needs direct network access to a new post office on another Windows server, you must map a drive to the post office directory before you start the MTA.

NOTE: The Linux MTA requires TCP/IP links to the POA.

To avoid these direct network access requirements between the MTA and a new post office, you can use TCP/IP links between the domain and the new post office.

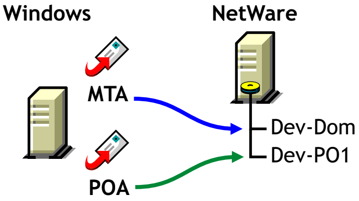


When using TCP/IP links, the MTA does not write message files into message queues in the post office directory structure. Instead, the MTA communicates the information to the POA by way of TCP/IP and then the POA uses its direct network access to write the information.

Cross-Platform Issues

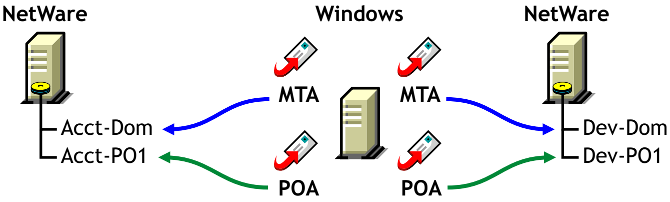
In most cases, it is most efficient if you match the POA platform with the network operating system where the post office resides. For example, if you create a new post office on a NetWare server, use the NetWare POA.

If you decide not to run the POA on the same platform as the post office, the POA must still have direct network access to the post office directory so that it can write to user databases (user*xxx*.db) and message databases (msg*nn*.db). For example, you could set up the new post office on a NetWare server and run the Windows POA on an Windows server to service it.



However, the NetWare POA could not service a post office located on an Windows server because Windows does not support the required cross-platform connection.

If you are using mapped or UNC links to the new post office, the MTA must also have direct network access to the post office directory so that it can write message files into the post office message queues. You could, for example, run the agents on an Windows server while domains and post offices were located on NetWare servers.



Again, the opposite combination of NetWare agents servicing domains and post offices on Windows servers is not an option because Windows does not support the required cross-platform connection.

To avoid these cross-platform access issues, use TCP/IP links between a domain and its post offices.

For more detailed information, see "Cross-Platform Issues between Domains and Post Offices" on page 561.

Deciding How to Link the New Post Office

When you create a new post office, you have the opportunity to choose the type of link to use between the new post office and its domain. Based on issues discussed in the preceding section, you might decide to set up a TCP/IP link between the new post office and its domain.

WORKSHEET

Under Item 14: Link to Domain, indicate the type of link you plan to set up between the new post office and its domain.

Selecting the Post Office Language

The post office language determines how times, dates, and numbers are displayed in the GroupWise client and determines the sorting rules for items in the GroupWise Address Book.

The post office defaults to the same language as its domain unless you specify otherwise. For example, if you set the domain and post office language to English-US, all time, date, and numbers are formatted according to English-US standards, and the Address Book items are sorted according to English-US sort order rules. This is true even if some users on the post office are running non-English GroupWise clients such as German or Japanese. Their client interface and Help files would be in German or Japanese, but the Address Book sort order would be according to English-US standards. Time, date, and number formats for the non-English clients defaults to the workstation language. Status tracking information depends on the language of the POA for the post office.

WORKSHEET

Under Item 5: Post Office Language, specify the post office language.

Selecting the Post Office Time Zone

When a message is sent from a user in one time zone to a user in another time zone, GroupWise adjusts the message's time so that it is correct for the recipient's time zone. For example, if a user in New York (GMT -05:00, Eastern Time) schedules a user in Los Angeles (GMT -08:00, Pacific Time) for a conference call at 4:00 p.m. Eastern Time, the appointment is scheduled in the Los Angeles user's calendar at 1:00 p.m. Pacific Time.

The domain time zone becomes the default time zone for each post office in the domain.

WORKSHEET

Under Item 6: Time Zone, specify the time zone for the new post office.

Selecting a Software Distribution Directory

A software distribution directory was created when your GroupWise system was initially set up. The software distribution directory contains files that users need in order to set up the GroupWise Windows or Cross-Platform client on their workstations. Additional software distribution directories might have been created since that time to accommodate users in various locations.

You can select the most convenient software distribution directory for the new post office.

WORKSHEET

Under Item 7: Software Distribution Directory, specify the name of the software distribution directory from which users in the new post office will install the GroupWise client software on their Windows, Linux, or Macintosh workstations.

Selecting a Post Office Security Level

Post office security settings affect two types of GroupWise users:

- Users who do not set passwords on their mailboxes
- Users who use LDAP passwords instead of GroupWise passwords to access their mailboxes

After a user sets a GroupWise password on his or her mailbox, the post office security level no longer applies. The user is always prompted for the password unless the administrator has set certain client options in ConsoleOne to prevent the password prompt, as described in "Managing GroupWise Passwords" on page 1034.

In the absence of passwords on users' mailboxes, the post office security level takes effect. By default, a new post office is created with low security. In a low security post office, mailboxes are completely unprotected. Without a password, any user's mailbox could be accessed by another user who knows how to use the @u-*userID* startup switch.

By increasing the post office security level to high, you provide protection to GroupWise mailboxes through other types of passwords. In a high security post office, you can choose between eDirectory authentication and LDAP authentication:

- **eDirectory Authentication:** If you use eDirectory authentication for a post office, users must be logged in to eDirectory in order to access their GroupWise mailboxes. Users cannot access other users' mailboxes unless they know the other users' network passwords.
- **LDAP Authentication:** If you use LDAP authentication for a post office, users must be successfully authenticated to an LDAP server before they can access their GroupWise mailboxes.

WORKSHEET

Under Item 11: Post Office Security Level, mark the security level for the post office. If you choose high security, indicate the type of authentication you plan to use.

Deciding if You Want to Create a Library for the New Post Office

If you anticipate that users on this post office will require document management services, you can create a library at the same time you create the post office. The library will be created with all of the default library options including Store Documents at Post Office. Using a document storage area is preferable to storing documents at the post office because a document storage area can be moved. You should appropriately configure the library immediately after it is created, before users begin to store documents there. See "Libraries and Documents" on page 261.

WORKSHEET

Under Item 8: Create Library, indicate whether or not you want to immediately create a library for the new post office. You can always add a library to the post office at a later time.

Setting Up the New Post Office

You should have already reviewed "Planning a New Post Office" on page 148 and filled out the "Post Office Worksheet" on page 163. Complete the following tasks to create a new post office.

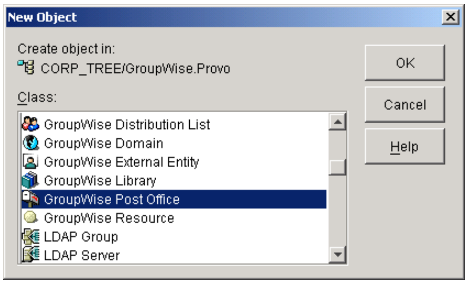
- "Creating the New Post Office" on page 158
- "Configuring the POA for the New Post Office" on page 161
- "Installing and Starting the New POA" on page 161
- "Setting Up User Access to the New Post Office" on page 162
- "What's Next" on page 162

Creating the New Post Office

1 Make sure you are logged in to the tree where you want to create the post office.

This must be the same tree as the domain that the post office belongs to (worksheet item 3).

2 In ConsoleOne, browse to and right-click the eDirectory container where you want to create the post office (worksheet item 1), then click New > Object.

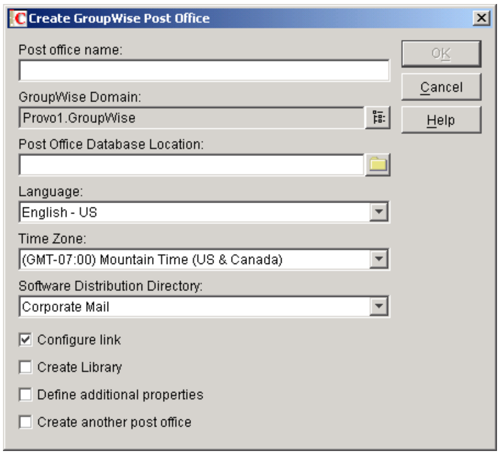


New Object

Create object in:
CORP_TREE/GroupWise.Provo

Class: GroupWise Post Office

3 Double-click GroupWise Post Office, then fill in the fields in the Create GroupWise Post Office dialog box (worksheet items 2 through 8).



Create GroupWise Post Office

Post office name:

GroupWise Domain: Provo1.GroupWise

Post Office Database Location:

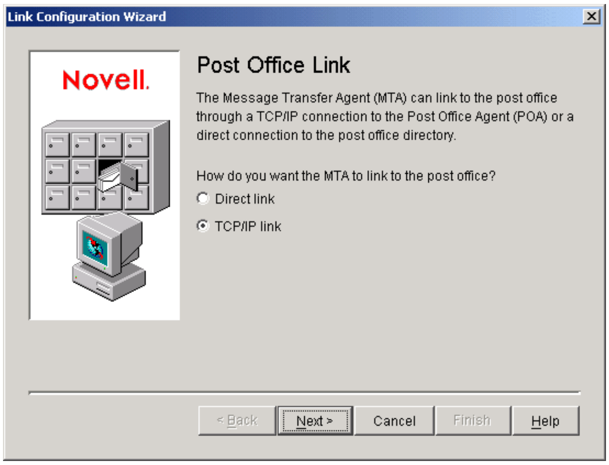
Language: English - US

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Software Distribution Directory: Corporate Mail

☑ Configure link
□ Create Library
□ Define additional properties
□ Create another post office

4 Make sure the Configure Links and Define Additional Properties options are selected, then click OK to display the Link Configuration Wizard.


Link Configuration Wizard

Post Office Link

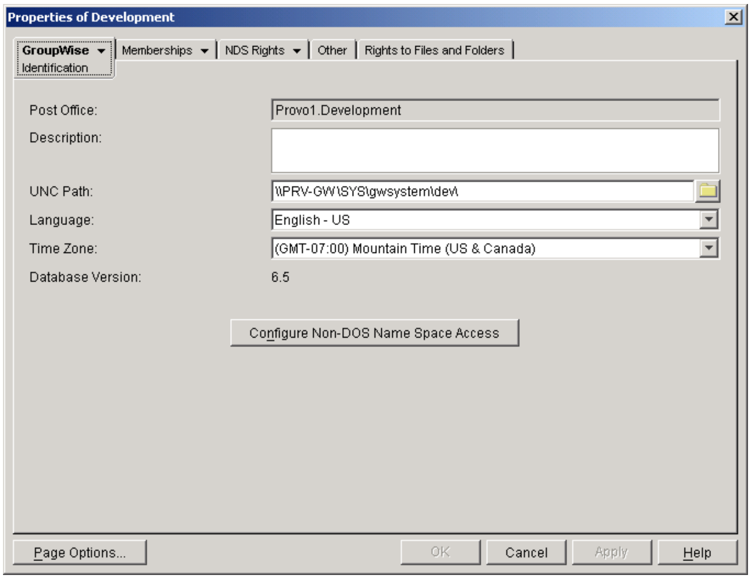
The Message Transfer Agent (MTA) can link to the post office through a TCP/IP connection to the Post Office Agent (POA) or a direct connection to the post office directory.

How do you want the MTA to link to the post office?

○ Direct link

● TCP/IP link

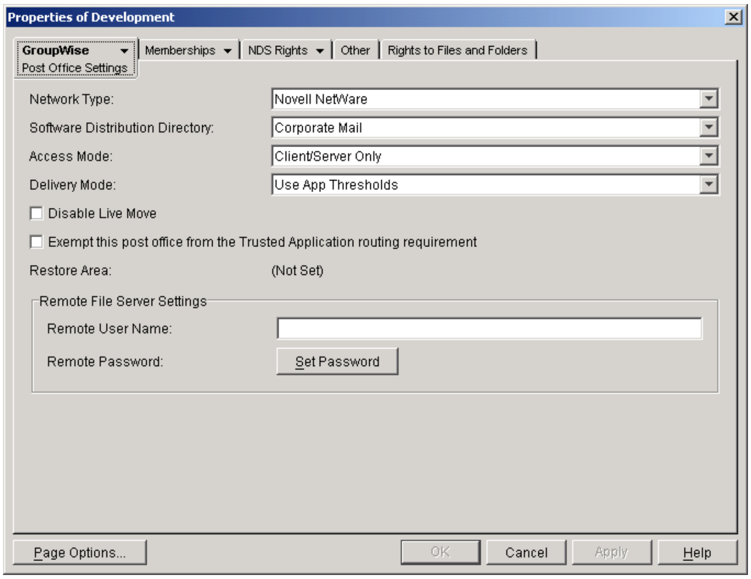
5 Follow the on-screen instructions to define how the post office links to its domain. When you've finished defining the link, ConsoleOne creates the Post Office object and displays the post office Identification page.


Properties of Development

Post Office:	Provo1.Development
Description:	
UNC Path:	\\PRV-GW\SYS\gwsystem\dev\
Language:	English - US
Time Zone:	(GMT-07:00) Mountain Time (US & Canada)
Database Version:	6.5

6 Fill in the Description field (worksheet item 9).

7 Click GroupWise > Post Office Settings to display the Post Office Settings page.



Network Type: Novell NetWare

Software Distribution Directory: Corporate Mail

Access Mode: Client/Server Only

Delivery Mode: Use App Thresholds

□ Disable Live Move

□ Exempt this post office from the Trusted Application routing requirement

Restore Area: (Not Set)

Remote File Server Settings

Remote User Name:

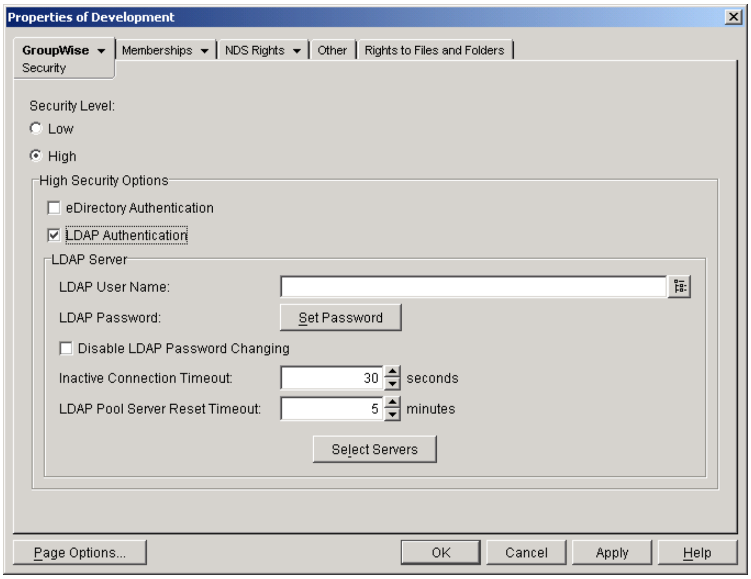
Remote Password:

8 Provide the network type for the post office location (worksheet item 10).

9 Select the software distribution directory for the post office (worksheet item 7).

10 If the POA will run on a different server from where the post office directory, a library, or a document storage area is located, provide a username and password that enables the POA to access the remote location (worksheet item 12).

11 Click GroupWise > Security to display the Security page.



Security Level:

○ Low

● High

High Security Options

□ eDirectory Authentication

☑ LDAP Authentication

LDAP Server

LDAP User Name:

LDAP Password:

□ Disable LDAP Password Changing

Inactive Connection Timeout: 30 seconds

LDAP Pool Server Reset Timeout: 5 minutes

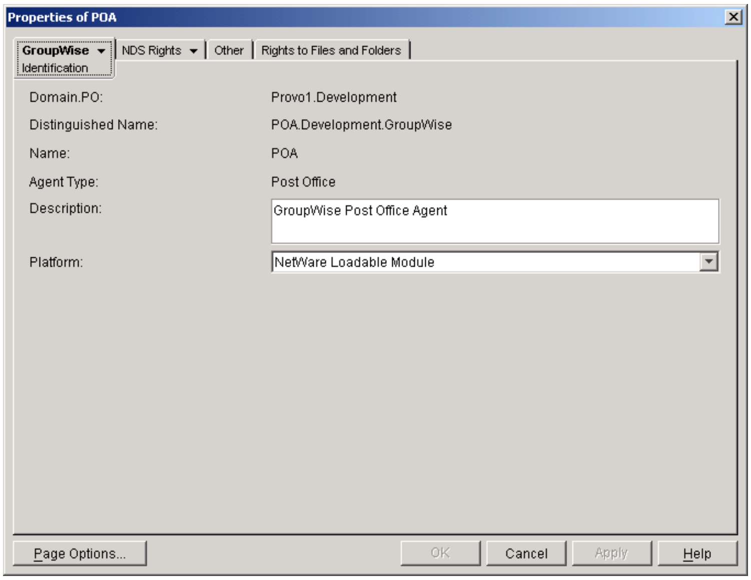
12 Provide the post office security level and authentication type for the post office (worksheet item 11). For additional LDAP instructions, see “Providing LDAP Authentication for GroupWise Users” on page 461.

13 Click OK to save the post office information.

Configuring the POA for the New Post Office

Although there are many POA settings, the default settings are sufficient to get your post office operational. However, there are a few important settings that you can conveniently modify before you install the agent software.

1. In ConsoleOne, double-click the new Post Office object.
2. Right-click the POA object, then click Properties to display the POA Identification page.



Domain.PO: Provo1.Development

Distinguished Name: POA.Development.GroupWise

Name: POA

Agent Type: Post Office

Description: GroupWise Post Office Agent

Platform: NetWare Loadable Module

3. Enter a description for the POA.

   The description displays on the POA agent console as the POA runs.
4. Select the platform where the POA will run (worksheet item 12).
5. If you have created the post office in a clustered environment, follow the instructions in the appropriate section of the GroupWise 6.5 Interoperability Guide:
   - "Installing and Configuring the MTA and the POA in a Cluster" in "Novell Cluster Services"
   - "Installing and Configuring the MTA and the POA in a Cluster" in "Microsoft Clustering Services"
6. For more POA configuration options, see "Changing POA Configuration to Meet Post Office Needs" on page 185.
7. Click OK to save the POA configuration information.

Installing and Starting the New POA

To install the POA for the new post office to the location recorded under worksheet item 11, follow the instructions in "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

Setting Up User Access to the New Post Office

The post office access mode determines how GroupWise client users access their mailboxes. By default, the GroupWise Windows and Cross-Platform clients use client/server access to the post office. Client/server access provides the following benefits:

- Client/server access provides the greatest level of security. Users do not need rights to the post office directory because the GroupWise client does not write directly to databases in the post office. All database updates are performed by the POA.
- Client/server access eliminates the need for separate network logins and passwords. This avoids problems with login restrictions, changing passwords, and insufficient network rights.
- Client/server access allows the GroupWise client to maintain multiple simultaneous connections to the post office.
- With client/server access mode, proxy rights can be granted to any user visible in the Address Book.

Historical Note: In GroupWise 5.*x*, the GroupWise client allowed the user to enter a path to the post office directory to facilitate direct access mode. The GroupWise 6.*x* client no longer offers the user that option. However, you can force the GroupWise 6.*x* client to use direct access mode by starting it with the /ps switch and providing the path to the post office directory. For information about alternatives to client/server access mode, see the *GroupWise 5.5 Agent Setup Guide* (http://www.novell.com/documentation/gw55/index.html).

Continue with "What's Next" on page 162.

What's Next

After you have created the new post office and started its POA, you are ready to expand the post office by:

- Adding users to the post office. See "Users" on page 187.
- Defining groups of users (distribution lists) that GroupWise users can select when addressing messages. See "Distribution Lists, Groups, and Organizational Roles" on page 235.
- Defining resources (for example, conference rooms or company cars) that users can schedule. See "Resources" on page 221.
- Defining libraries and setting up Document Management Services. See "Libraries and Documents" on page 261.
- Setting up the GroupWise Windows or Cross-Platform client software so that GroupWise users can run the client from Windows, Linux, or Macintosh workstations. See "Client" on page 963.
- Configuring the POA for optimal performance. See "Post Office Agent" on page 415.

Post Office Worksheet

Use this worksheet as you complete the tasks in "Planning a New Post Office" on page 148.

Item	Explanation
1) eDirectory Container	Specify the name of the eDirectory container where you plan to create the new post office. For more information, see "Determining the Context for the Post Office Object" on page 150.
2) Post Office Name	Specify a name for the new post office. Choose the name carefully. After the post office is created, it cannot be renamed. For more information, see "Choosing the Post Office Name" on page 151.
3) GroupWise Domain	Specify the domain this post office will belong to. For more information, see "Selecting the Domain That the Post Office Will Belong To" on page 149.
4) Post Office Database Location	Specify the path for the post office directory. Choose the post office directory carefully. After it is created, it is difficult to rename. For more information, see "Deciding Where to Create the Post Office Directory" on page 152.
5) Post Office Language	Specify the post office language if it is different from the domain language. For more information, see "Selecting the Post Office Language" on page 156.
6) Post Office Time Zone	Specify the time zone for the post office if it is different from the domain time zone. For more information, see See "Selecting the Post Office Time Zone" on page 156.
7) Software Distribution Directory:	Specify the name of the software distribution directory for the new post office. For more information, see "Selecting a Software Distribution Directory" on page 156.
8) Create Library: ◆ Yes ◆ No	Mark whether or not you want to create a library for the new post office at the same time you create the new post office. For more information, see "Deciding if You Want to Create a Library for the New Post Office" on page 157.
9) Post Office Description	Enter a description for the new post office to help you identify its function in the system.
10) Network Type	Specify the network type in use on the server where the new post office will be located. For more information, see "Deciding Where to Create the Post Office Directory" on page 152.
11) Post Office Security Level: ◆ Low ◆ High - eDirectory authentication - LDAP authentication	Mark the security level for the post offices. For high security, mark the type of authentication you plan to use. For more information, see "Selecting a Post Office Security Level" on page 157.

Item	Explanation
12) Agent Location ◆ POA on the same server as the post office (local) ◆ POA on a different server from the post office (remote) - Username - Password	Mark the location of the POA relative to the post office. If the POA will run on a different server from where the post office, a library, or a document storage area is located, provide a username and password to enable the POA to access the remote location. For more information, see "Deciding Where to Install the Agent Software" on page 153.
13) Agent Platform ◆ NetWare POA ◆ Linux POA ◆ Windows POA	Specify the platform where you plan to run the POA. For more information, see "Deciding Where to Install the Agent Software" on page 153.
14) Link to Domain ◆ TCP/IP ◆ Mapped ◆ UNC	Mark how you plan to link the new post office to its domain. For more information, see "Deciding How to Link the New Post Office" on page 156.

12 Managing Post Offices

As your GroupWise® system grows and evolves, you might need to perform the following maintenance activities on post offices:

- "Connecting to the Domain That Owns a Post Office" on page 165
- "Editing Post Office Properties" on page 166
- "Managing Disk Space Usage in the Post Office" on page 171
- "Auditing Mailbox License Usage in the Post Office" on page 180
- "Tracking and Restricting Client Access to the Post Office" on page 181
- "Disabling a Post Office" on page 183
- "Moving a Post Office" on page 183
- "Deleting a Post Office" on page 184
- "Changing POA Configuration to Meet Post Office Needs" on page 185

See also "Maintaining Domain and Post Office Databases" on page 345 and "Backing Up GroupWise Databases" on page 375. Proper database maintenance and backups allow recovery from accidental deletions, as described in "Restoring Deleted Mailbox Items" on page 381 and "Recovering Deleted GroupWise Accounts" on page 384.

Connecting to the Domain That Owns a Post Office

Whenever you change post office information, it is most efficient to connect directly to the domain that the post office belongs to before you begin making modifications. Performing administrative tasks on a post office while not connected to the post office's domain increases the amount of administrative message traffic sent between domains.

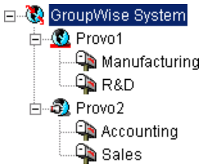
To change your domain connection:

1 In ConsoleOne® in the Console View, click Tools > GroupWise System Operations. Click Select Domain, browse to and select the domain directory, then click OK.

   or

   In the GroupWise View, right-click the Domain object, then click Connect.

   The GroupWise view identifies the domain that you are connected to by adding a plug symbol to the domain icon.

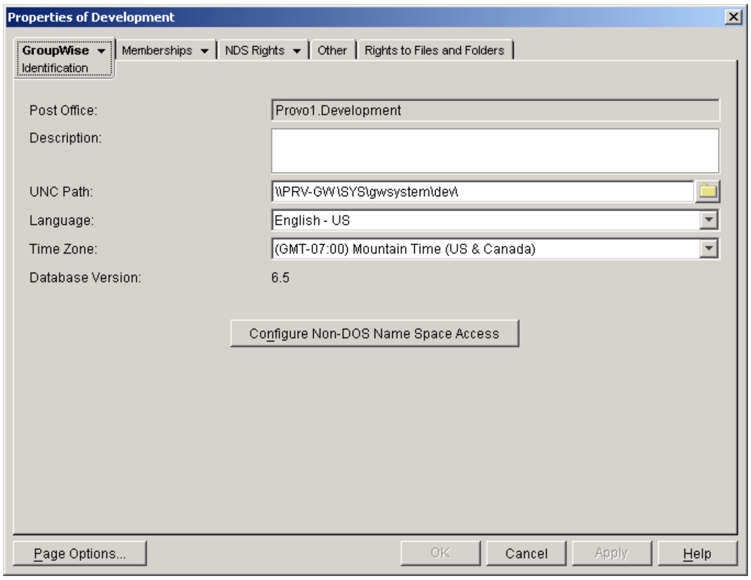


   The domain marked with the red underscore is the primary domain.

Editing Post Office Properties

After creating a post office, you can change some post office properties. Other post office properties cannot be changed.

1 In ConsoleOne, browse to and right-click the Post Office object, then click Properties to display the post office Identification page.


Properties of Development
GroupWise
Identification
Memberships
NDS Rights
Other
Rights to Files and Folders
Configure Non-DOS Name Space Access
Page Options...
OK
Cancel
Apply
Help

Post Office: Provo1.Development

Description:

UNC Path: \\PRV-GW\SYS\gwsystem\dev\

Language: English - US

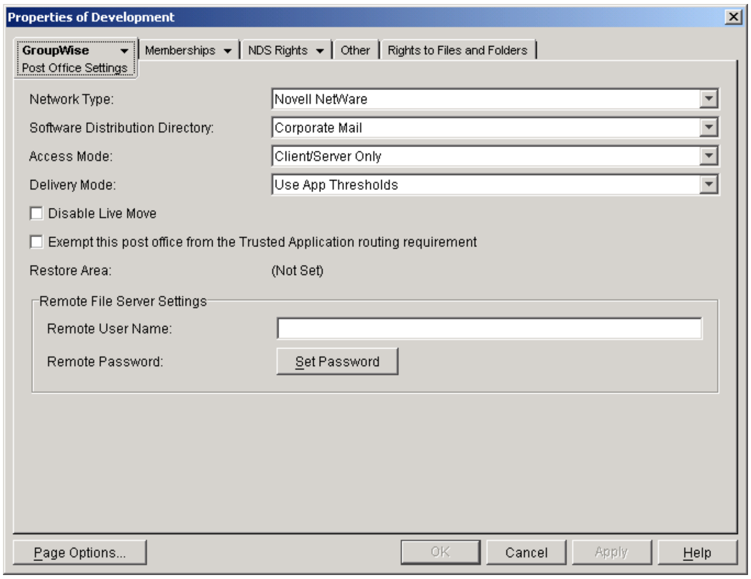
Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Database Version: 6.5

2 Change editable fields as needed.

For information about individual fields, see "Setting Up the New Post Office" on page 158 or use online help when editing the post office.

3 Click GroupWise > Post Office Settings to display the Post Office Settings page.



Network Type: Novell NetWare

Software Distribution Directory: Corporate Mail

Access Mode: Client/Server Only

Delivery Mode: Use App Thresholds

□ Disable Live Move

□ Exempt this post office from the Trusted Application routing requirement

Restore Area: (Not Set)

Remote File Server Settings

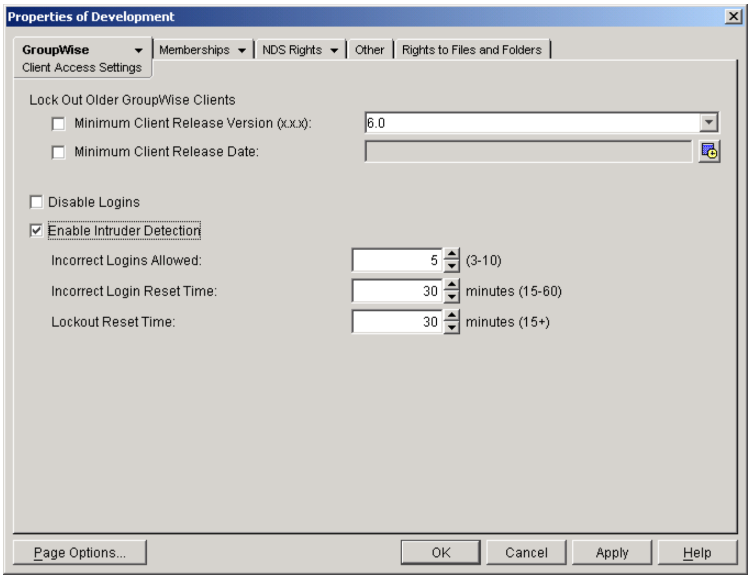
Remote User Name:

Remote Password:

These post office settings are discussed in the following sections:

- “Selecting a Software Distribution Directory” on page 156
- “Setting Up User Access to the New Post Office” on page 162

4 Click GroupWise > Client Access Settings to display the Client Access Settings page.



Lock Out Older GroupWise Clients

☐ Minimum Client Release Version (x.x.x): 6.0

☐ Minimum Client Release Date:

☐ Disable Logins

☑ Enable Intruder Detection

Incorrect Logins Allowed: 5 (3-10)

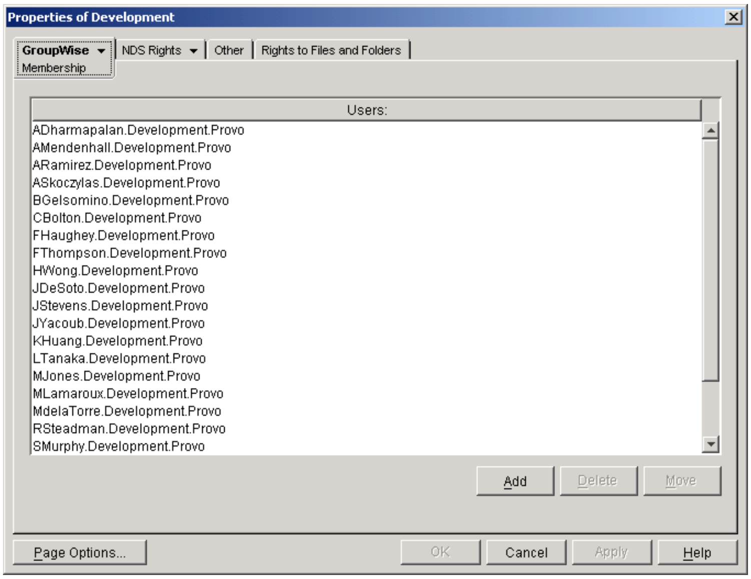
Incorrect Login Reset Time: 30 minutes (15-60)

Lockout Reset Time: 30 minutes (15+)

The client access settings are discussed in the following sections:

- “Tracking and Restricting Client Access to the Post Office” on page 181
- “Disabling a Post Office” on page 183
- “Enabling Intruder Detection” on page 465

5 Click GroupWise > Membership to display the Membership page.

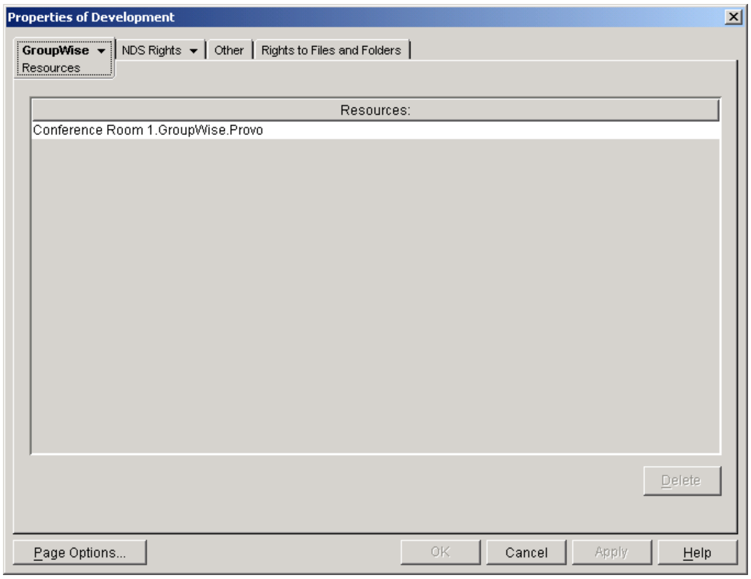


Users:

ADharmapalan.Development.Provo
AMendenhall.Development.Provo
ARamirez.Development.Provo
ASkoczylas.Development.Provo
BGelsomino.Development.Provo
CBolton.Development.Provo
FHaughey.Development.Provo
FThompson.Development.Provo
HWong.Development.Provo
JDeSoto.Development.Provo
JStevens.Development.Provo
JYacoub.Development.Provo
KHuang.Development.Provo
LTanaka.Development.Provo
MJones.Development.Provo
MLamaroux.Development.Provo
MdelaTorre.Development.Provo
RSteadman.Development.Provo
SMurphy.Development.Provo

All users in the post office are listed, no matter where their Novell® eDirectory™ objects are located in the tree. Here you can add, delete, and move users in the post office. See “Users” on page 187.

6 Click GroupWise > Resources to display the Resources page.

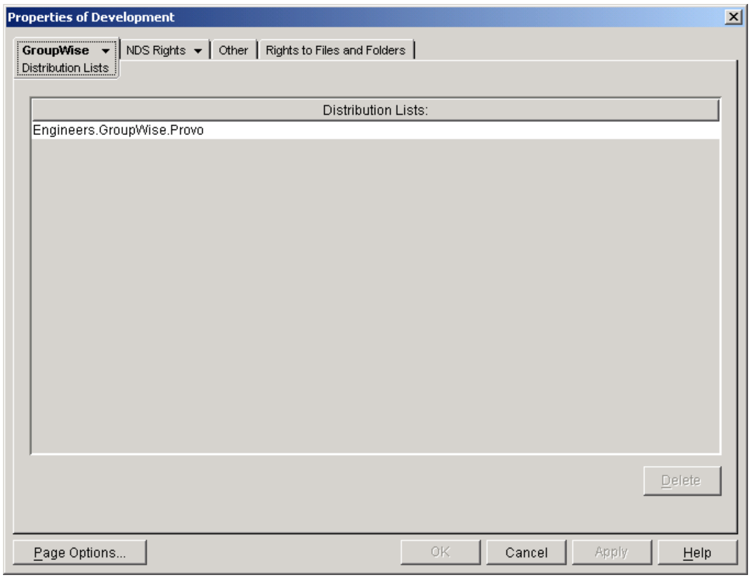


Properties of Development

Resources:
Conference Room 1.GroupWise.Provo

All resources in the post office are listed, no matter where their eDirectory objects are located in the tree. This is a convenient place to delete resources from the post office. See "Resources" on page 221

7 Click GroupWise > Distribution Lists to display the Distribution Lists page.

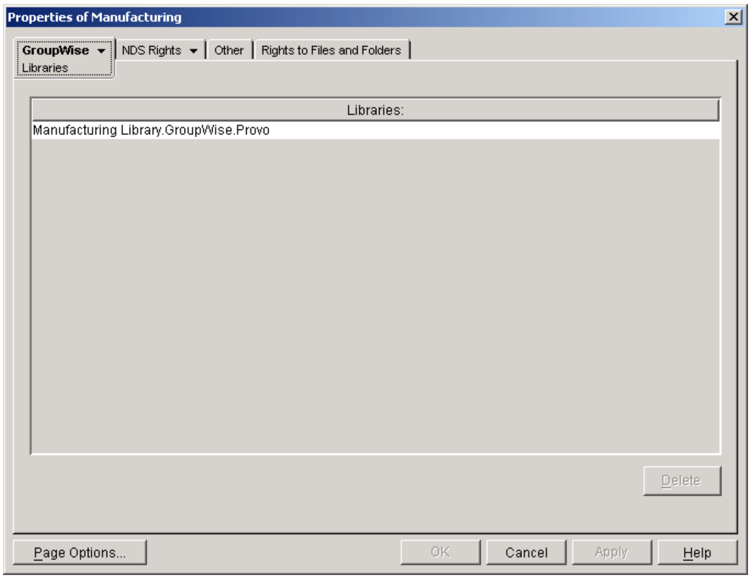


Properties of Development

Distribution Lists:
Engineers.GroupWise.Provo

All distribution lists in the post office are listed, no matter where their eDirectory objects are located in the tree. This is a convenient place to delete distribution lists from the post office. See "Distribution Lists, Groups, and Organizational Roles" on page 235.

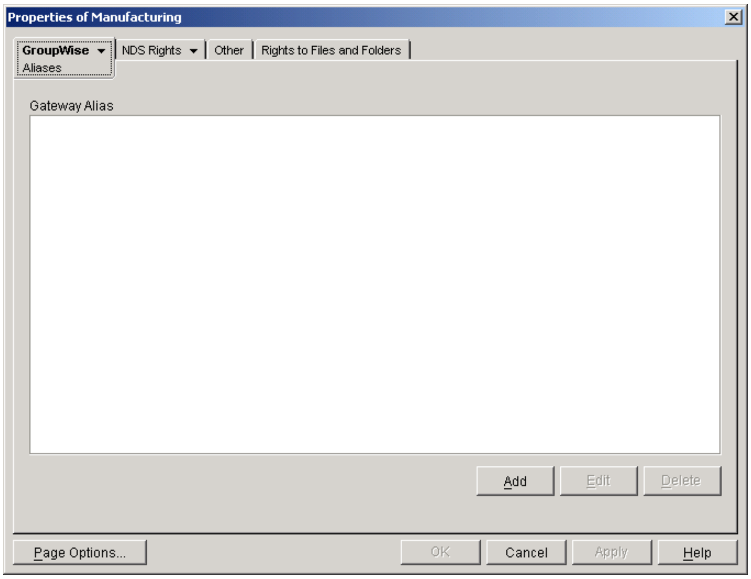
8 Click GroupWise > Libraries to display the Libraries page.



Libraries:
Manufacturing Library.GroupWise.Provo

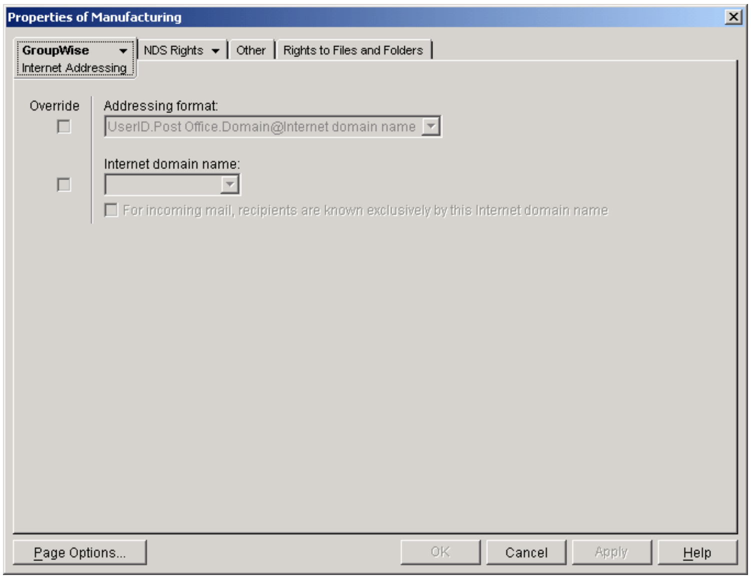
All libraries belonging to the post office are listed, no matter where their eDirectory objects are located in the tree. This is a convenient place to delete libraries. See "Libraries and Documents" on page 261.

9 Click GroupWise > Aliases to display the Aliases page.



You need to set up aliases for a post office only if you are using GroupWise gateways. For a list of gateways, see GroupWise 6.*x* Gateways (http://www.novell.com/documentation/gw6xgate/index.html). GroupWise 5.5 gateways can be used with GroupWise 6.5.

10 Click GroupWise > Internet Addressing to display the Internet Addressing page.



Override

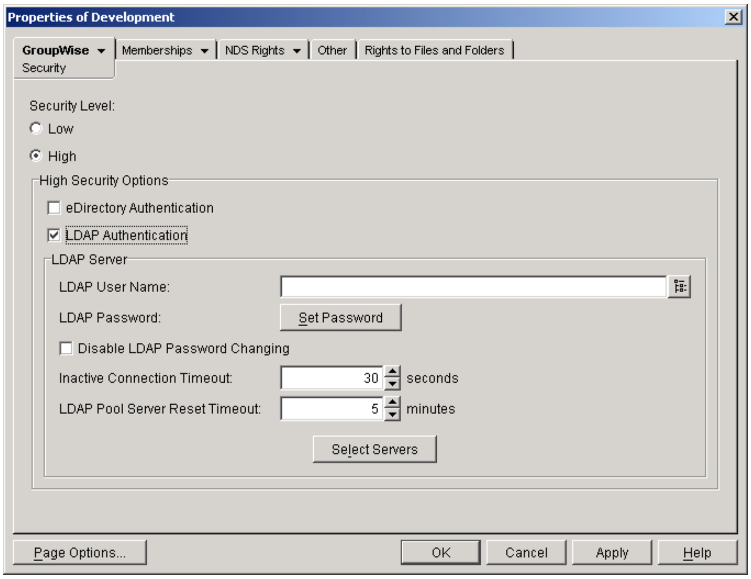
□ Addressing format: UserID.Post Office.Domain@Internet domain name

□ Internet domain name:

□ For incoming mail, recipients are known exclusively by this Internet domain name

Here you provide information used to determine the Internet addressing settings for the post office. See “Internet-Style Addressing” on page 87 for more information.

11 Click GroupWise > Security to display the Security page.



Security Level:

○ Low

● High

High Security Options

□ eDirectory Authentication

☑ LDAP Authentication

LDAP Server

LDAP User Name:

LDAP Password:

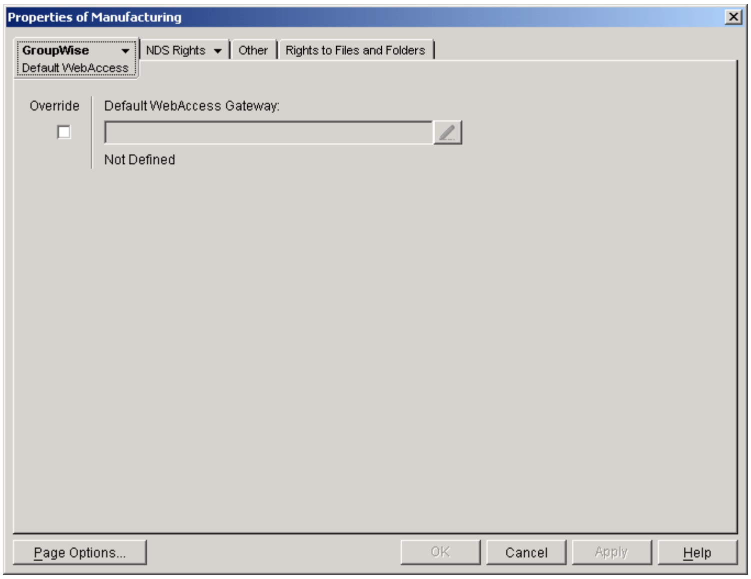
□ Disable LDAP Password Changing

Inactive Connection Timeout: 30 seconds

LDAP Pool Server Reset Timeout: 5 minutes

For instructions on setting the security level for the post office, see “Selecting a Post Office Security Level” on page 157.

12 Click GroupWise > Default WebAccess to display the Default WebAccess page.



Override

□

Default WebAccess Gateway:

Not Defined

Use this page to designate the default WebAccess gateway for the post office. See "WebAccess" on page 803 for more information.

13 Click OK to save changes to the post office properties.

Managing Disk Space Usage in the Post Office

Many users are prone to save every message and attachment they ever receive. You can moderate this behavior by implementing disk space management:

- "Preparing to Implement Disk Space Management" on page 171
- "Setting Mailbox Size Limits" on page 172
- "Enforcing Mailbox Size Limits" on page 174
- "Restricting the Size of Messages That Users Can Send" on page 175
- "Preventing the Post Office from Running Out of Disk Space" on page 176
- "An Alternative to Disk Space Management in the Post Office" on page 179

NOTE: The Cross-Platform client does not currently respect the mailbox size limits established in ConsoleOne.

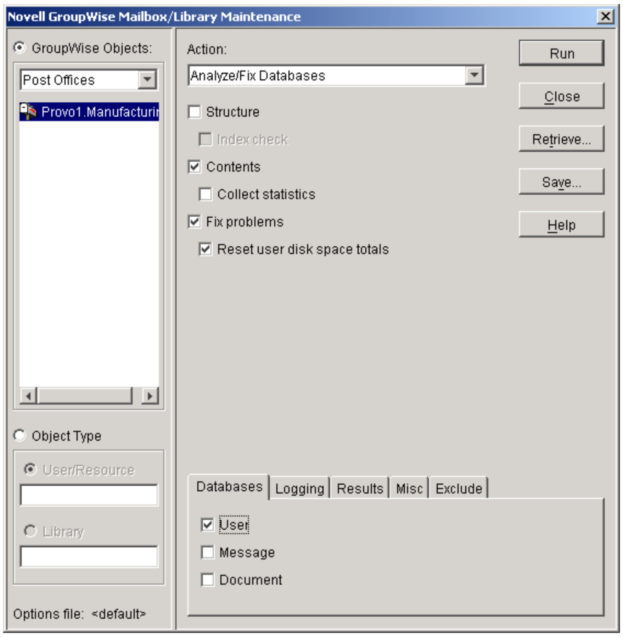
Preparing to Implement Disk Space Management

If you are implementing disk space management in an existing GroupWise system, you must begin by setting the initial size information on all users' mailboxes. If you are implementing disk space management in a new GroupWise system, skip to "Setting Mailbox Size Limits" on page 172.

To establish current mailbox size:

1 In ConsoleOne, browse to and select a Post Office object.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.


Novell GroupWise Mailbox/Library Maintenance

● GroupWise Objects:
Post Offices
Provo1.Manufacturi

○ Object Type
● User/Resource
○ Library

Options file: <default>

Action: Analyze/Fix Databases

☐ Structure
☐ Index check
☑ Contents
☐ Collect statistics
☑ Fix problems
☑ Reset user disk space totals

☑ User
☐ Message
☐ Document

3 In the GroupWise Objects field, select Post Offices.

4 In the Action field, select Analyze/Fix Databases.

5 As options to the action, select Contents, Fix Problems, and Reset User Disk Space Totals. Make sure all other options are deselected.

6 On the Databases tab, select User. Make sure all other types of databases are deselected.

7 Click Run > OK to acknowledge that the Mailbox/Library Maintenance task has been sent to the POA.

After the POA has performed the task, current mailbox size information becomes available on each user's mailbox. The information is updated regularly as the user receives and deletes messages.

8 To generate a report of current mailbox information, follow the instructions in "Gathering Mailbox Statistics" on page 367.

9 Repeat Step 1 through Step 8 for each post office where you want to implement disk space management.

10 Continue with "Setting Mailbox Size Limits" on page 172.

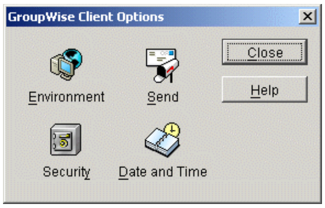
Setting Mailbox Size Limits

After initial size information is recorded on each user's mailbox, you can establish a limit on the amount of disk space each user's mailbox is allowed to occupy. You can set a single limit for an entire domain. You can set different limits for each post office. You can even set individual user limits if necessary.

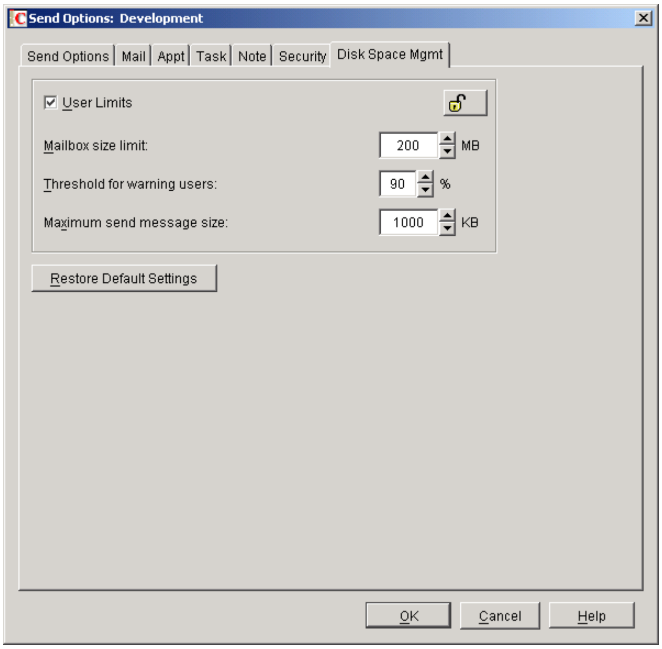
If you are implementing disk space management in an existing GroupWise system where users are accustomed to unlimited disk space, you should warn them about the coming change. After you establish the mailbox size limits as described in this section, users whose mailboxes exceed the established limit cannot send messages until the size of their mailboxes is reduced. Users might want to manually delete and archive items in advance in order to avoid this interruption in their use of GroupWise.

To establish mailbox size limits:

1. In ConsoleOne, browse to and select a Domain, Post Office, or User object.
2. Click Tools > GroupWise Utilities > Client Options.



3. Click Send > Disk Space Management.



☑ User Limits

Mailbox size limit: 200 MB

Threshold for warning users: 90 %

Maximum send message size: 1000 KB

4. Select User Limits.
5. Specify the maximum number of megabytes allowed for each user’s mailbox.

   Unless disk space is extremely limited, 200 MB is a comfortable mailbox size to enforce.
6. Specify as a percentage the point where you want to warn users that their mailboxes are getting full.

   After a user receives a warning message, he or she cannot send additional messages until mailbox cleanup has been performed and the mailbox size is brought below the warning percentage.
7. Optionally, specify in kilobytes the largest message that users can send.

   By restricting message size, you can influence how fast users’ mailboxes fill up. However, if users have valid reasons for sending messages that exceed this limit, the limit can become a hindrance to users getting their work done.
8. Click OK > Close to save the disk space management settings.

9 If you are adding disk space management to an existing GroupWise system where users' mailboxes are already over the desired size limit, continue with "Enforcing Mailbox Size Limits" on page 174.

or

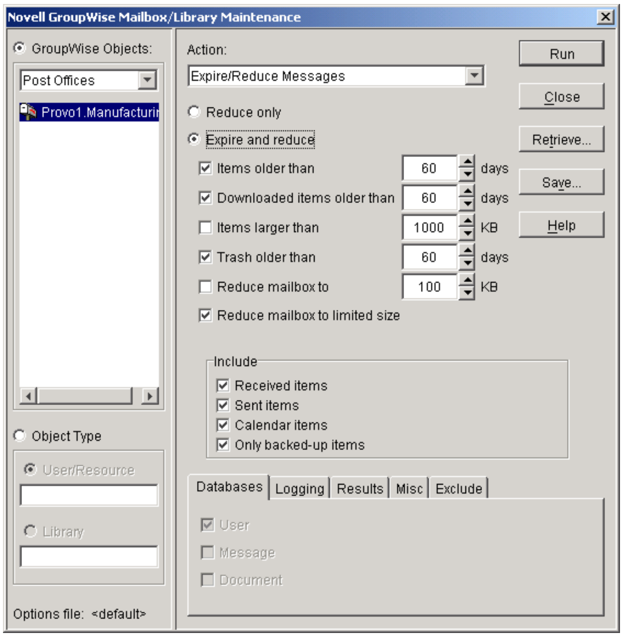
If you are implementing disk space management in a new system where users have not yet begun to use their mailboxes, see "Using Mailbox Storage Size Information" in "Managing Your Mailbox" in the *GroupWise 6.5 Windows Client User Guide* to see how setting a mailbox size limit affects users' activities in the GroupWise client.

Enforcing Mailbox Size Limits

If existing GroupWise users are having difficulty fitting their mailboxes into the established mailbox size limits, you can assist them by reducing their mailboxes for them. Users should be warned before this action is taken.

1 In ConsoleOne, select a Post Office object.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.


Novell GroupWise Mailbox/Library Maintenance

● GroupWise Objects: Post Offices

Provo1.Manufacturi

○ Object Type

○ User/Resource

○ Library

Options file: <default>

Action: Expire/Reduce Messages

○ Reduce only

● Expire and reduce

☑ Items older than 60 days

☑ Downloaded items older than 60 days

☐ Items larger than 1000 KB

☑ Trash older than 60 days

☐ Reduce mailbox to 100 KB

☑ Reduce mailbox to limited size

Include

☑ Received items

☑ Sent items

☑ Calendar items

☑ Only backed-up items

Databases: ☑ User ☐ Message ☐ Document

3 In the Action field, select Expire/Reduce.

4 Set the Expire and Reduce options as desired, making sure that Reduce Mailbox to Limited Size is selected.

5 Click Run > OK to acknowledge that the Mailbox/Library Maintenance task has been sent to the POA.

After the POA has performed the task, users mailboxes fit within the mailbox size limit you have established.

6 Repeat Step 1 through Step 5 for each post office where you want to reduce users' mailboxes to the established mailbox size limit.

See "Using Mailbox Storage Size Information" in "Managing Your Mailbox" in the *GroupWise 6.5 Windows Client User Guide* to see how setting a mailbox size limit affects user's activities in the GroupWise client.

Restricting the Size of Messages That Users Can Send

By restricting message size, you can influence how fast users' mailboxes fill up. However, if users have valid reasons for sending messages that exceed this limit, the limit can become a hindrance to users getting their work done.

There are three levels at which you can restrict message size:

- "Within the Post Office" on page 175
- "Between Post Offices" on page 176
- "Between Domains" on page 176
- "Between Your GroupWise System and the Internet" on page 176

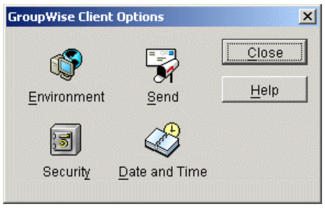
NOTE: Although the Cross-Platform client does not respect the message size limits established in ConsoleOne using Tools > GroupWise Utilities > Client Options > Send > Disk Space Management, messages originating from the Cross-Platform client can be restricted by the POA and MTA as they pass between post offices and domains.

Within the Post Office

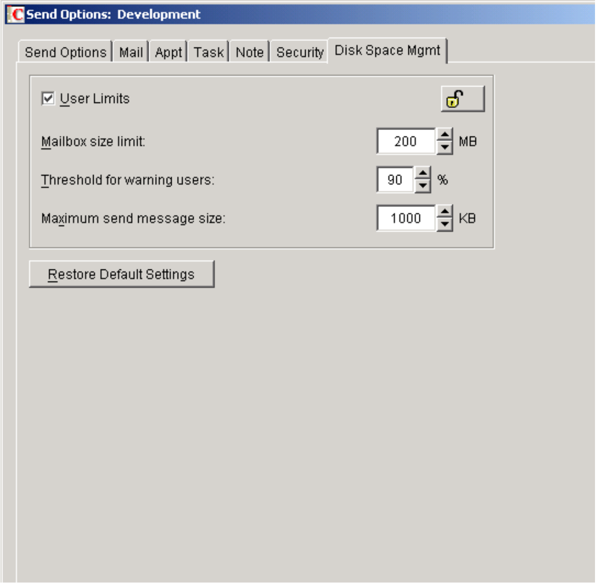
You can use Client Options to restrict the size of messages that users can send within their local post office.

1 In ConsoleOne, browse to and select a Domain, Post Office, or User object.

2 Click Tools > GroupWise Utilities > Client Options.



3 Click Send > Disk Space Management.



☑ User Limits

Mailbox size limit: 200 MB

Threshold for warning users: 90 %

Maximum send message size: 1000 KB

4 Select User Limits.

5 Specify in kilobytes the largest message that users can send.

6 Click OK > Close to save the maximum message size setting.

Between Post Offices

You can configure the POA to restrict the size of messages that it allows to pass outside the local post office. See "Restricting Message Size between Post Offices" on page 455 for setup instructions.

Between Domains

You can configure the MTA to restrict the size of messages that it allows to pass outside the local domain. See "Restricting Message Size between Domains" on page 588 for setup instructions.

Between Your GroupWise System and the Internet

You can configure the Internet Agent to restrict the size of messages that it allows to pass outside your GroupWise system. See "Controlling User Access" on page 705 for setup instructions.

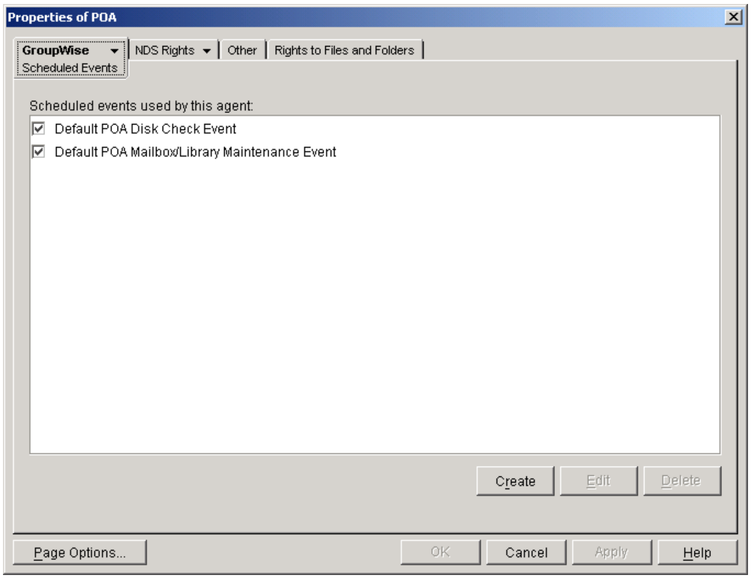
Preventing the Post Office from Running Out of Disk Space

In spite of the best disk space management plans, it is still possible that some unforeseen situation could result in a post office running out of disk space. To prevent this occurrence, you can configure the POA to stop processing messages, so that disk space usage in the post office cannot increase until the disk space problem is resolved.

1 In ConsoleOne, double-click a Post Office object, right-click its POA object, then click Properties.

2 Click GroupWise > Agent Settings, then adjust the settings in the Disk Check Interval and Disk Check Delay fields as described in "Scheduling Disk Space Management" on page 469.

3 Click GroupWise > Scheduled Events.

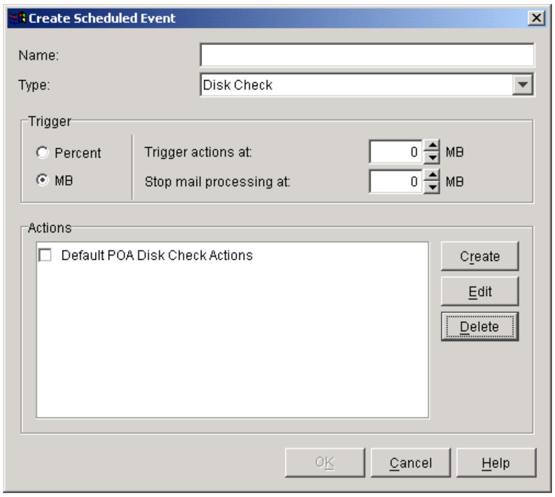


Scheduled events used by this agent:

☑ Default POA Disk Check Event

☑ Default POA Mailbox/Library Maintenance Event

4 Click Create to create a new scheduled event to handle an unacceptably low disk space condition.


Create Scheduled Event

Name:

Type: Disk Check

Trigger

○ Percent

● MB

Trigger actions at: 0 MB

Stop mail processing at: 0 MB

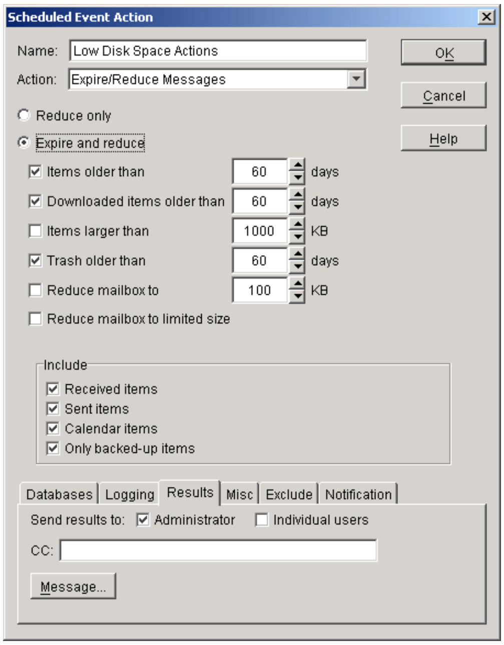
Actions

□ Default POA Disk Check Actions

5 Type a unique name for the new scheduled event, then select Disk Check as the event type.

6 In the Trigger Actions At field, specify the amount of free post office disk space at which to take preventive measures.

7 Click Create to define your own disk check actions, then give the new action a unique name.


Scheduled Event Action

Name: Low Disk Space Actions

Action: Expire/Reduce Messages

○ Reduce only

● Expire and reduce

☑ Items older than	60	days
☑ Downloaded items older than	60	days
□ Items larger than	1000	KB
☑ Trash older than	60	days
□ Reduce mailbox to	100	KB

□ Reduce mailbox to limited size

Include

☑ Received items

☑ Sent items

☑ Calendar items

☑ Only backed-up items

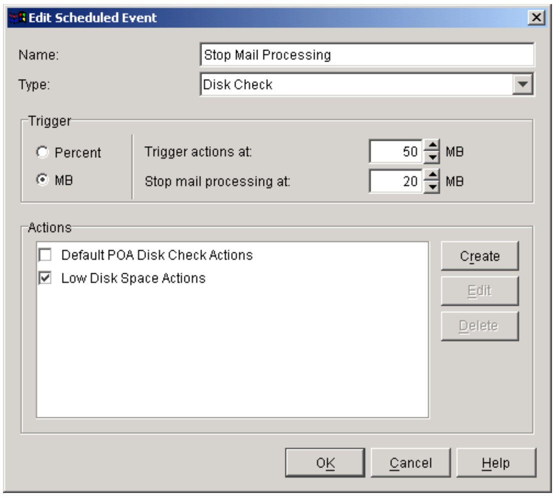
Send results to: ☑ Administrator □ Individual users

CC:

8 Configure the actions for the POA to take in order to relieve the low disk space condition.

Use the Results or Notification tab if you want to receive notification about the POA's response to the low disk space condition.

9 Click OK to return to the Create Scheduled Event dialog box.



Name: Stop Mail Processing

Type: Disk Check

Trigger

○ Percent

● MB

Trigger actions at: 50 MB

Stop mail processing at: 20 MB

Actions

□ Default POA Disk Check Actions

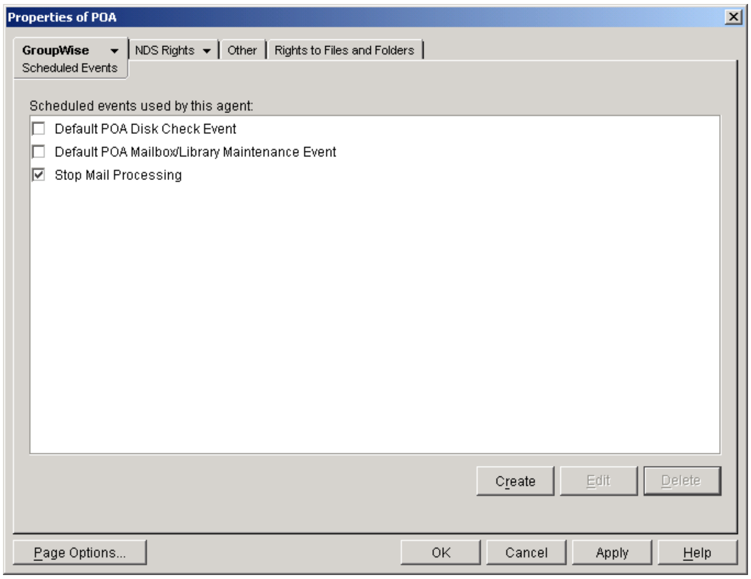
☑ Low Disk Space Actions

For additional instructions, see "Scheduling Disk Space Management" on page 469.

10 Select the new set of actions.

11 In the Stop Mail Processing At field, specify the amount of free post office disk space at which you want the POA to stop processing messages.

12 Click OK to create the new disk space management event and return to the Scheduled Events page.



Scheduled events used by this agent:

□ Default POA Disk Check Event

□ Default POA Mailbox/Library Maintenance Event

☑ Stop Mail Processing

13 Select the new disk space management event.

14 Click OK to close the Scheduled Events page.

ConsoleOne then notifies the POA to restart so the new disk space management event can be put into effect.

An Alternative to Disk Space Management in the Post Office

If you want to place more responsibility for disk space management onto GroupWise client users, you can require that they run the client in Caching mode, where all messages can be stored on users' workstations, or other personal locations, rather than in the post office. For an overview of Caching mode, see:

- "Using Caching Mode" in the *GroupWise 6.5 Windows Client User Guide*
- "Using Caching Mode" in the *GroupWise 6.5 Cross-Platform Client User Guide*

IMPORTANT: Do not force Caching mode for a post office that supports Outlook clients along with GroupWise clients.

Forcing Caching Mode

You can force Caching mode for an entire domain. You can force Caching mode for specific post offices. You can even force Caching mode for an individual user if necessary.

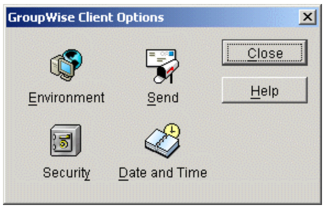
When you initially force caching mode, users' Caching mailboxes are identical with their Online mailboxes. However, as you employ disk space management processes in the post office and reduce the size of users' Online mailboxes, more and more of the users' mailbox items exist only in their Caching mailboxes. Make sure that users understand their responsibilities to back up their Caching mailboxes, as described in:

- "Backing Up Your Mailbox" in "Managing Your Mailbox" in the *GroupWise 6.5 Windows Client User Guide*
- "Backing Up Your Mailbox" in "Managing Your Mailbox" in the *GroupWise 6.5 Cross-Platform Client User Guide*

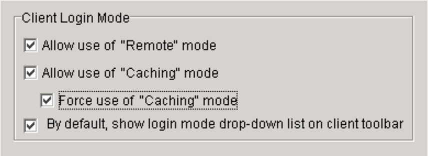
To force Caching mode:

1 In ConsoleOne, browse to and select a Domain, Post Office, or User object.

2 Click Tools > GroupWise Utilities > Client Options.



3 Click Environment > General.



Client Login Mode

☑ Allow use of "Remote" mode

☑ Allow use of "Caching" mode

☑ Force use of "Caching" mode

☑ By default, show login mode drop-down list on client toolbar

4 In the Client Login Mode box, select Force Use of Caching Mode.

5 Click OK > Close to save the Caching mode setting.

If you are helping existing users, who might have sizeable mailboxes, to start using Caching mode exclusively, you can configure the POA to respond efficiently when multiple users need to download their entire mailboxes for the first time. See "Supporting Forced Mailbox Caching" on page 454 for setup instructions.

Auditing Mailbox License Usage in the Post Office

You can run an audit report on a post office to see 1) which mailboxes require full client licenses and which mailboxes require limited client licenses, and 2) which mailboxes are active (have been accessed at least one time), which ones have never been active, and which ones have been inactive for a specified period of time.

A mailbox requires a full client license (and is marked as a full client license mailbox) if it has been accessed by any of the following:

- The GroupWise Windows client (grpwise.exe)
- GroupWise Notify (notify.exe) or GroupWise Address Book (addrbook.exe)
- The GroupWise Cross-Platform client (groupwise)
- A third-party plug-in to the GroupWise client API
- The Microsoft Outlook Plug-In for GroupWise 5.5
- Microsoft Outlook with the GroupWise client for Windows installed

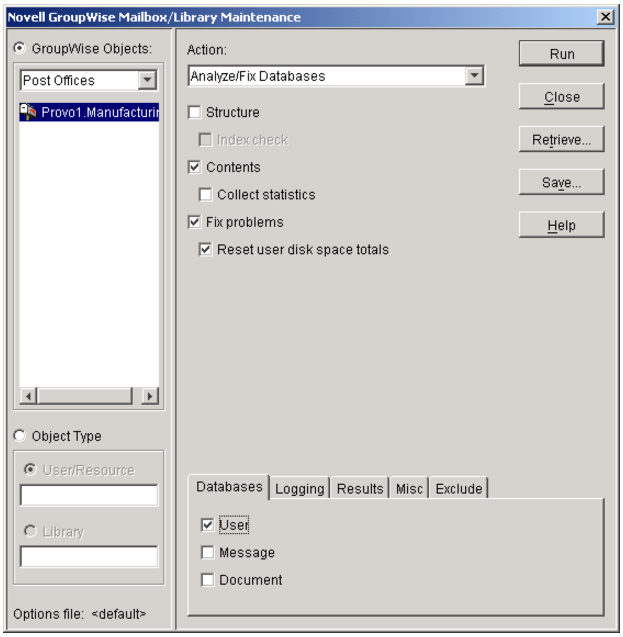
A mailbox requires a limited client license only (and is marked as a limited client license mailbox) if access to it has been limited to the following:

- The GroupWise WebAccess client (including wireless devices)
- A GroupWise Windows or WebAccess client via the Proxy feature
- Any GroupWise client via the Busy Search feature
- A POP or IMAP client

To generate an audit report for the post office:

1 In ConsoleOne, browse to and select the Post Office object.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



Novell GroupWise Mailbox/Library Maintenance

● GroupWise Objects: Post Offices

Provo1.Manufacturi

○ Object Type

○ User/Resource

○ Library

Options file: <default>

Action: Analyze/Fix Databases

□ Structure

□ Index check

☑ Contents

□ Collect statistics

☑ Fix problems

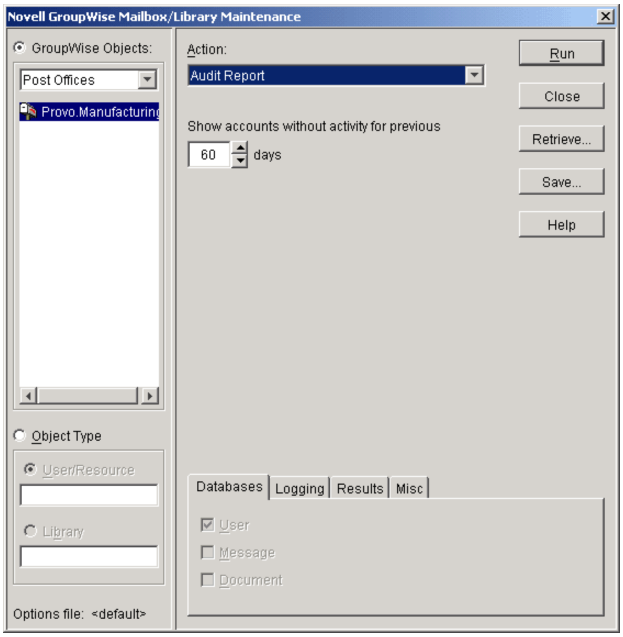
☑ Reset user disk space totals

☑ User

□ Message

□ Document

3 In the Action field, select Audit Report.



Novell GroupWise Mailbox/Library Maintenance

● GroupWise Objects: Post Offices

Provo.Manufacturing

Action: Audit Report

Show accounts without activity for previous 60 days

○ Object Type

● User/Resource

○ Library

☑ User

☐ Message

☐ Document

Options file: <default>

4 In the Show Accounts without Activity for *nn* Days field, select the number of days you want to use for the inactivity report.

Using the default setting (60 days) causes the Mailbox/Library Maintenance program to indicate the mailboxes that have not had any activity within the last 60 days.

5 If you want write the report to a log file, click the Logging tab, then specify a name for the log file.

6 If you want to send the results as an e-mail message to the domain's GroupWise administrator or to another individual, click the Results tab, then select the appropriate options.

7 Click Run > OK to acknowledge that the Mailbox/Library Maintenance task has been sent to the POA.

After the POA has performed the task, the audit report is generated in the format (log file or e-mail message) you specified.

Audit reports are stored as part of the information available on Post Office and Domain objects in ConsoleOne. Right-click a Domain or Post Office object, then click Tools > GroupWise Diagnostics > Information. The information stored on the Domain object is cumulative for all post office in the domain for which audit reports have been run.

Audit reports can also be scheduled to run on a regular basis by properly configuring the POA to perform a Mailbox/Library Maintenance event. See "Scheduling Database Maintenance" on page 467.

Tracking and Restricting Client Access to the Post Office

By default, the post office allows multiple versions of the GroupWise Windows and Cross-Platform clients to access it. Using the Web console available for the post office's POA, you can see the version number of each GroupWise client that logs in to the post office in client/server access mode (TCP/IP to the POA). This information is displayed on the POA Web console's C/S Users page. For more information, see "Using the POA Web Console" on page 489.

IMPORTANT: Because the POA provides the version tracking and enforces the client lockout, this functionality applies only to GroupWise clients that are accessing the post office in client/server mode (not direct access mode).

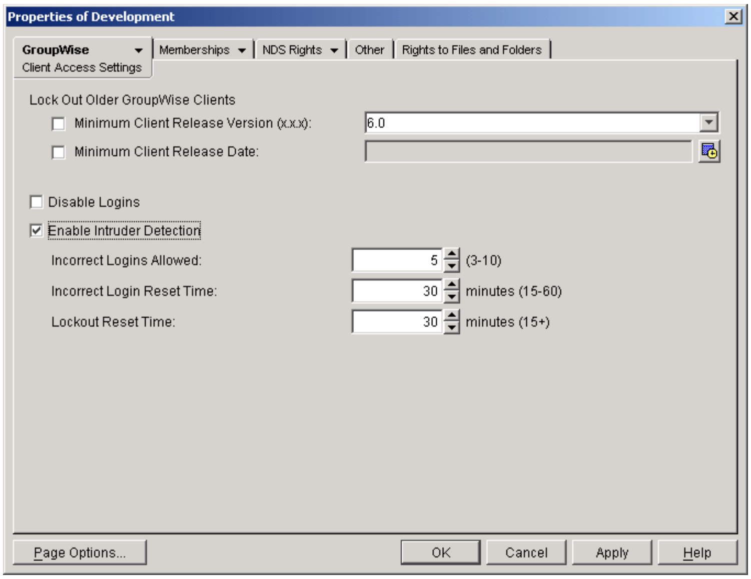
To help you better monitor and track which versions of the GroupWise client are being used to access the post office, you can specify a preferred GroupWise client version for the post office. Any version that does not match the preferred version is highlighted on the POA Web console's C/S Users page. Older versions are shown in red, and newer versions are shown in blue.

In addition, to restrict which versions of the GroupWise client can access the post office, you can choose to lock out any GroupWise clients that are older than the preferred version. If you want to lock out all GroupWise clients (for example, to rebuild the post office database), see "Disabling a Post Office" on page 183.

To specify a preferred GroupWise client version for the post office and to enable the POA to lock out specific GroupWise client versions:

1 In ConsoleOne, right-click the Post Office object, then click Properties.

2 Click GroupWise > Client Access Settings to display the Client Access Settings page.



Lock Out Older GroupWise Clients

□ Minimum Client Release Version (x.x.x): 6.0

□ Minimum Client Release Date:

□ Disable Logins

☑ Enable Intruder Detection

Incorrect Logins Allowed: 5 (3-10)

Incorrect Login Reset Time: 30 minutes (15-60)

Lockout Reset Time: 30 minutes (15+)

3 Fill in the following fields:

Minimum Client Release Version: Enter the version to use as the post office's preferred GroupWise client version. Any version that does not match the preferred version is highlighted on the POA Web console's C/S Users page. Older versions are shown in red, and newer versions are shown in blue. The version number syntax should match what is displayed in the GroupWise client's About GroupWise dialog box. Only version 5.5 Enhancement Pack SP1 and newer are supported.

Minimum Client Release Date: This field is available only if you specify a release version. You can use this field to associate an expected release date with the release version. The C/S Users page would highlight any dates that do not match the one entered here.

Lock Out Older GroupWise Clients: Select this option for either or both of the above options to lock out any GroupWise clients (client/server mode only) that are older than the version and/or date specified in the Release Version and Release Date fields. For example, if you entered 6.0.0 in the Release Version field and April 6, 2001 12:00 AM in the Release Date field and selected this option for both, any GroupWise client that is older than version 6.0 or is dated before April 6, 2001 12:00 AM would not be allowed access to the post office.

4 Click OK to save the changes.

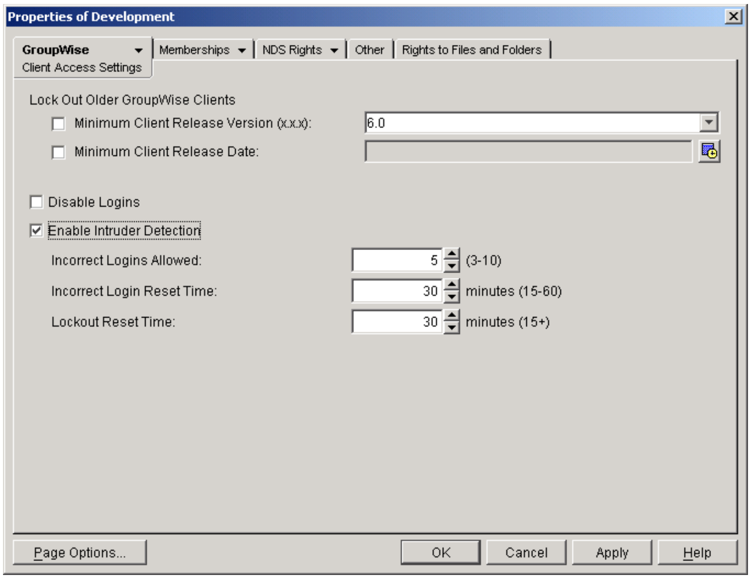
Disabling a Post Office

Disabling a post office restricts users from starting the GroupWise Windows or Cross-Platform client and accessing the post office. However, users who are already running the GroupWise client can continue to access the post office; after they exit, they cannot access the post office again until the post office is enabled.

A post office must be disabled if you are rebuilding the post office database (wphost.db). You might also want to disable a post office when you are doing a complete GroupWise system backup. That ensures that all data is consistent at the time of the backup.

1 In ConsoleOne, browse to and right-click the Post Office object, then click Properties.

2 Click GroupWise > Client Access Settings to display the Client Access Settings page.



Properties of Development

Lock Out Older GroupWise Clients

□ Minimum Client Release Version (x.x.x): 6.0

□ Minimum Client Release Date:

□ Disable Logins

☑ Enable Intruder Detection

Incorrect Logins Allowed: 5 (3-10)

Incorrect Login Reset Time: 30 minutes (15-60)

Lockout Reset Time: 30 minutes (15+)

3 Select Disable Logins, then click OK to disable the post office.

4 To re-enable logins, deselect Disable Logins so that it is blank.

Moving a Post Office

You cannot move a Post Office object in ConsoleOne because it is a container object. Only leaf objects can be moved. If you need to change the context, graft the GroupWise post office to its corresponding eDirectory object in the new container location. See “GW / eDirectory Association” on page 73 for more information on grafting objects.

You can, however, move the post office directory, the post office database (wphost.db), and the other databases that reside in the post office by copying the post office directory structure and all its contents to the new location.

IMPORTANT: Follow these instructions if you want to move a post office on a NetWare or Windows server to another directory on the same server or to a different NetWare or Windows server. If you want to move a post office located on a NetWare or Windows server onto a Linux server, see "Moving a Post Office to Linux" in "Update" in the *GroupWise 6.5 Installation Guide*.

To move a post office directory structure and all its contents:

1. Make sure all users are out of the post office, then disable logins to the post office. See "Disabling a Post Office" on page 183.
2. Back up the post office. See Chapter 31, "Backing Up GroupWise Databases," on page 375.
3. In ConsoleOne, display the Identification page of the post office to move.
4. In the UNC Path field, change the UNC path to the location where you want to move the post office, then click OK to save the new location.

   The location change is then propagated up to the domain.
5. Stop the POA for the post office.
6. Use xcopy with the /s and /e options to move the post office directory and its contents. These options re-create the same directory structure even if directories are empty.

   Example: `xcopy` *`post_office_directory`* `/s /e` *`destination`*
7. Give rights to objects that need to access the post office database.

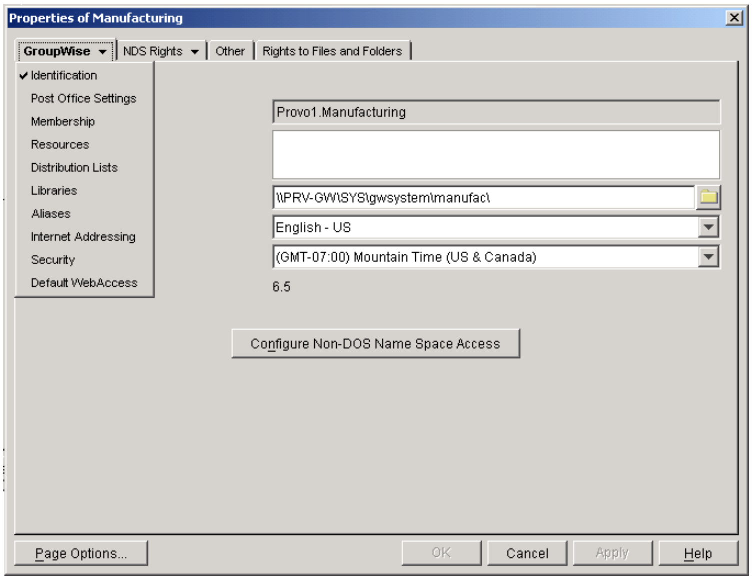
   For example, the NetWare® POA needs rights if the new location is on a different server.
8. Edit the POA startup file by changing the setting of the /home switch, then restart the POA. See "Adjusting the POA for a New Post Office Location" on page 445.
9. When you are sure the post office is functioning properly, delete the original post office directories.

If you need to move the POA along with its post office, see "Moving the POA to a Different server" on page 445.

Deleting a Post Office

You cannot delete a post office until you have deleted or moved all objects that belong to it.

1. In ConsoleOne, right-click the Post Office object to delete, then click Properties.



Provo1.Manufacturing

\\PRV-GW\SYS\gwsystem\manufac\

English - US

(GMT-07:00) Mountain Time (US & Canada)

6.5

2 Click GroupWise > Resources, then delete any resources that still belong to the post office. See "Deleting a Resource" on page 230.

You must delete resources before users, because users who own resources cannot be deleted without assigning a new owner in the same post office.

3 Click GroupWise > Membership, then delete or move any users that still belong to the post office. See "Removing GroupWise Accounts" on page 215 and "Moving GroupWise Accounts" on page 198.

4 Click GroupWise > Distribution Lists, then delete any distribution lists that still belong to the post office. See "Deleting a Distribution List" on page 244.

5 Click GroupWise > Libraries, delete any libraries that still belong to the post office. See "Deleting a Library" on page 299.

6 Click OK to perform the deletions.

It is easy to perform such deletions in the GroupWise View. Select the Post Office object in the GroupWise View, then use the drop-down list of objects to display objects of each type that still belong to the post office. Delete any residual objects in the Console View.

7 In ConsoleOne, browse to and right-click the Domain object that owns the post office to delete, then click Properties.

8 Click GroupWise > Post Offices, select the post office to delete, then click Delete.

9 Stop the POA for the post office and uninstall the POA software if applicable.

See "Stopping the POA" on page 480 and "Uninstalling the POA Software" on page 435.

Changing POA Configuration to Meet Post Office Needs

Because the POA delivers messages to mailboxes, responds in real time to client/server users, and maintains all databases located in the post office, its functioning affects the post office and all users who belong to the post office. Proper POA configuration is essential for a smoothly running GroupWise system. Complete details about the POA are provided in "Post Office Agent" on page 415. As you create and manage post offices, you should keep in mind the following aspects of POA configuration:

- "Enhancing Post Office Security with SSL Connections to the POA" on page 458
- "Providing LDAP Authentication for GroupWise Users" on page 461
- "Enabling Intruder Detection" on page 465
- "Supporting IMAP Clients" on page 450
- "Optimizing Client/Server Processing" on page 507
- "Scheduling Database Maintenance" on page 467
- "Performing Nightly User Upkeep" on page 472
- "Restricting Message Size between Post Offices" on page 455

IV Users

13 Creating GroupWise Accounts

For users to be able to use GroupWise®, you must give them GroupWise accounts. A GroupWise account defines the user in the GroupWise system by providing the user with a GroupWise user ID and GroupWise mailbox.

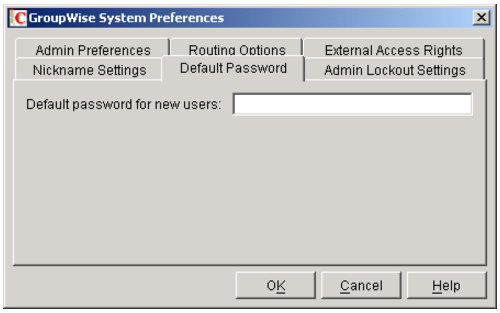
You can give GroupWise accounts to Novell® eDirectory™ users during or after their creation in eDirectory. You can also give GroupWise accounts to users who do not have eDirectory accounts. Refer to the following sections for details:

- "Establishing a Default Password for All New GroupWise Accounts" on page 189
- "Creating GroupWise Accounts for eDirectory Users" on page 190
- "Creating GroupWise Accounts for Non-eDirectory Users" on page 195
- "Educating Your New Users" on page 196

Establishing a Default Password for All New GroupWise Accounts

To save time and energy when you are creating new GroupWise accounts, you can establish a default password to use for all new accounts.

1 In ConsoleOne®, click Tools > GroupWise System Operations > System Preferences > Default Password.



Default password for new users:

2 Type the password you want to use as the default, then click OK.

3 Explain to users how to set their own passwords in the GroupWise client, as described in "Assigning Passwords to Your Mailbox" in the *GroupWise 6.5 Windows Client User Guide*.

Creating GroupWise Accounts for eDirectory Users

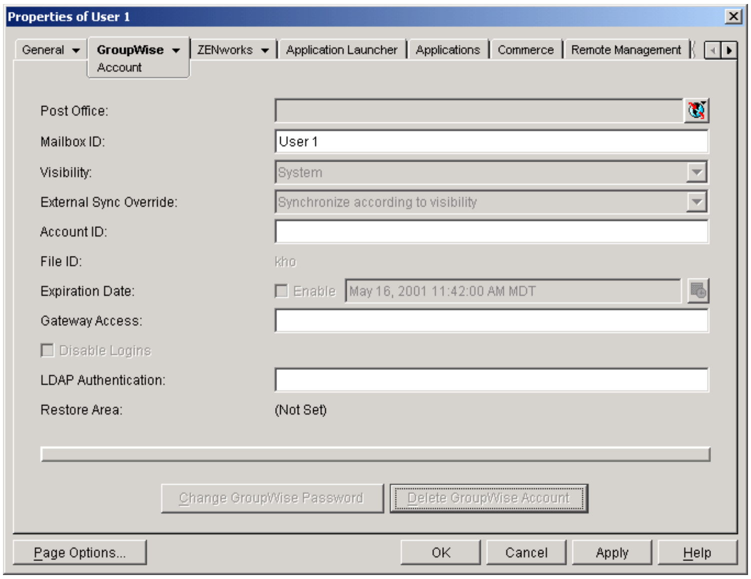
Depending on your needs, you can choose from the following methods to create GroupWise accounts for eDirectory users:

- Creating a Single GroupWise Account: You can create a GroupWise account for a single eDirectory user by editing the GroupWise information on his or her User object. This method lets you create the GroupWise account on any post office, select the GroupWise user ID, and configure optional GroupWise information. It provides the most flexibility in creating a user's GroupWise account.
- Creating Multiple GroupWise Accounts: You can create GroupWise accounts for multiple eDirectory users by editing the membership information on a Post Office object. This method allows you to quickly add multiple users to the same post office at one time. However, you cannot select the user's GroupWise user ID; instead, the user's eDirectory username is automatically used as his or her GroupWise user ID. In addition, to configure other optional GroupWise information for a user, you need to modify each User object.
- Creating GroupWise Accounts by Importing Users: You can import information from ASCII-delimited text files.
- Using a Template to Create GroupWise Accounts: You can create a template to apply to new eDirectory User objects you create. The template can be configured to automatically assign the user to a post office.

Creating a Single GroupWise Account

To create a GroupWise account for an eDirectory user:

1. In ConsoleOne, right-click the User object, then click Properties.
2. Click GroupWise > Account to display the Account page.



Post Office:

Mailbox ID: User 1

Visibility: System

External Sync Override: Synchronize according to visibility

Account ID:

File ID: kho

Expiration Date: □ Enable May 16, 2001 11:42:00 AM MDT

Gateway Access:

□ Disable Logins

LDAP Authentication:

Restore Area: (Not Set)

3. Fill in the following fields:

Post Office: Select the post office where you want the user's mailbox created.

Mailbox ID: The Mailbox ID (also referred to as the GroupWise user ID) defaults to the eDirectory username. You can change it if necessary.

IMPORTANT: GroupWise mailbox IDs cannot contain periods. If the eDirectory username contains one or more periods, you must provide a mailbox ID that does not contain periods.

4 Click Apply to create the account.

You must create the account by clicking Apply (or OK) before you can modify any of the other fields, including the GroupWise password.

5 If desired, modify any of the following optional fields:

Visibility: Select the level at which you want the user to be visible in the Address Book. System enables the user to be visible to all users in your GroupWise system. Domain enables the user to be visible to all users in the same domain as the user. Post Office enables the user to be visible to all users on the same post office as the user. Setting the visibility level to None means that no users will see the user in the Address Book. However, even if the user is not displayed in the Address Book, other users can send messages to the user by typing the user's ID (mailbox ID) in a message's To field.

External Sync Override: This option applies only if your GroupWise system links to and synchronizes with an external system.

Select the Synchronize According to Visibility setting if you want the user information to be provided to the other system only if the user's visibility is set to System.

Select the Synchronize Regardless of Visibility setting if you always want the user information provided to the other system regardless of the user's visibility level.

Select the Don't Synchronize Regardless of Visibility setting if you never want the user information provided to the other system.

Account ID: This option applies only if you have a GroupWise gateway that supports accounting. For more information about gateway accounting, see your GroupWise gateway documentation (http://www.novell.com/documentation/gw65/index.html).

File ID: This three-letter ID is randomly generated and is non-editable. It is used for various internal purposes within the GroupWise system, including ensuring that files associated with the user have unique names.

Expiration Date: If you want the user's GroupWise account to no longer work after a certain date, specify the expiration date. This date applies to the user's GroupWise account only; it is independent of the eDirectory account expiration date (User object > Restrictions tab > Login Restrictions page).

Gateway Access: This option applies only if you have GroupWise gateways that support access restrictions. For more information, see your gateway documentation (http://www.novell.com/documentation/gw6/index.html).

Disable Logins: Select this option to prevent the user from accessing his or her GroupWise mailbox.

LDAP Authentication: This option applies only if you are using LDAP to authenticate users to GroupWise (see "Providing LDAP Authentication for GroupWise Users" on page 461) and the LDAP server is not the Novell LDAP server. If this is the case, enter the user's LDAP authentication ID.

Restore Area: This field applies only if you are using the GroupWise backup and restore features. If so, this field indicates the location where the user's mailbox is being backed up. For details, see Chapter 32, "Restoring GroupWise Databases from Backup," on page 379.

Change GroupWise Password: Click this option to assign a password to the user's GroupWise account or change the current password. The user will be prompted for this password each time he or she logs in to GroupWise.

To be able to skip this option by setting a default password, see "Establishing a Default Password for All New GroupWise Accounts" on page 189.

Delete GroupWise Account: Click this option to delete the user's GroupWise account. This includes the user's mailbox and all items in the mailbox. The user's eDirectory account is not affected.

6 Click Apply to save the changes.

7 Click GroupWise > General > Identification to display the user's current eDirectory information.

This information will appear in the GroupWise Address Book, as described in Chapter , "Address Book," on page 81. If you keep private information in the Description field of the User object, you can prevent this information from appearing the GroupWise Address Book. See "Preventing the User Description Field from Displaying in the Address Book" on page 85.

8 Make sure that the user's eDirectory information is current, then click OK.

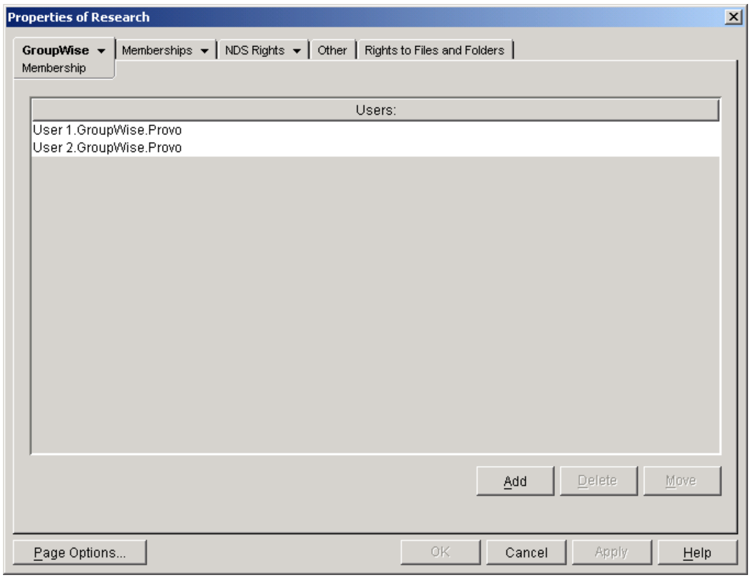
Creating Multiple GroupWise Accounts

If you have multiple eDirectory users who will have GroupWise accounts on the same post office, you can use the Post Office object's Membership page to quickly add the users and create their accounts. Each user's GroupWise user ID will be the same as his or her eDirectory username.

To create GroupWise accounts for multiple eDirectory users:

1 In ConsoleOne, right-click the Post Office object, then click Properties.

2 Click GroupWise > Membership to display the Membership page.

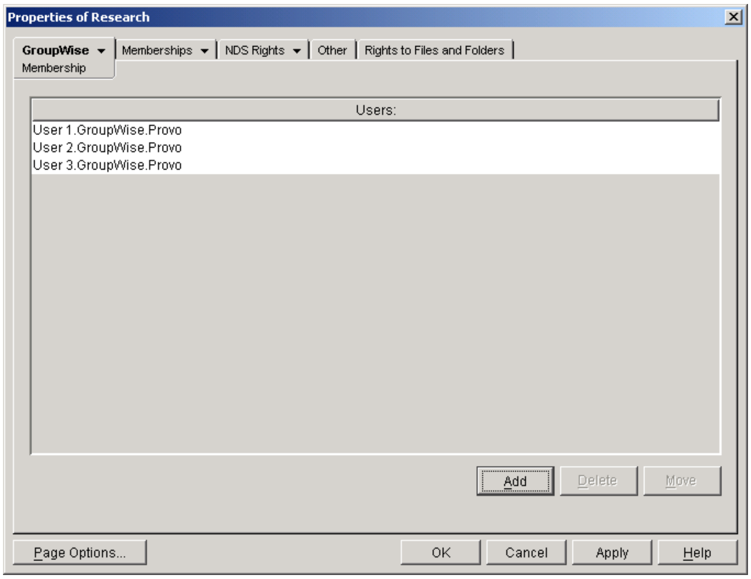


User 1.GroupWise.Provo
User 2.GroupWise.Provo

3 Click Add, select the eDirectory user you want to add to the post office, then click OK to add the user to the post office's membership list.

By default, the user’s eDirectory username is used as the GroupWise ID.

IMPORTANT: GroupWise IDs cannot contain periods. If the any of the eDirectory usernames contain periods, you must provide GroupWise IDs that do not contain periods on the GroupWise Account page of each User object.



User 1.GroupWise.Provo
User 2.GroupWise.Provo
User 3.GroupWise.Provo

4 Repeat Step 3 to create additional GroupWise accounts in the post office.

5 When finished, click OK to save the changes.

Creating GroupWise Accounts by Importing Users

You can quickly create multiple GroupWise users by importing ASCII-delimited text files created by the GroupWise Export utility or by a third-party export. The text files provide the eDirectory and GroupWise attributes necessary for creating users. For information about using the GroupWise Import utility, see “Import” on page 68. For information about using the GroupWise Export utility, see “Export” on page 71.

Using a Template to Create GroupWise Accounts

If you frequently create new users, you might want to create Template objects with the necessary GroupWise properties. This makes creating a new eDirectory user with GroupWise access a one-step process. However, you cannot use a Template object to give GroupWise properties to existing eDirectory users.

The steps to create a template with GroupWise properties include assigning the post office and setting up directory rights. Because a user can have membership in only one post office, a different template should be created for each existing post office. Further, for each post office, a template can be created for different categories of users, such as secretarial, accounting, administrative, human resources, development, sales, and manufacturing.

After one template has been created with eDirectory properties and post office directory rights, you can use it to quickly create templates for subsequent post offices.

- “Creating a Template” on page 194
- “Creating a User Account from a Template” on page 194

Creating a Template

1. In ConsoleOne, right-click the Organizational Unit object where you want to create the Template object, then click New > Object to display the New Object dialog box.

   Templates should be placed in the same organizational unit where they will be used because the browser first lists any templates in the current context. The template will also inherit rights from the container the template is created in, further simplifying its setup.

2. In the Class list, select Template, then click OK to display the New Template dialog box.
3. Enter a name that describes the purpose for which the template will be used.
4. If you want to base the template on another Template or User object, select Use Template or User, then browse to and select the desired Template or User object.
5. Select Define Additional Properties.
6. Click Create to display the properties pages for the Template object.
7. Click GroupWise > Information.
8. Fill in the following fields:

   Post Office: Select the post office the user will be assigned to.

   Visibility: Select the level at which the user will be visible in the Address Book. System enables the user to be visible to all users in your GroupWise system. Domain enables the user to be visible to all users in the same domain as the user. Post Office enables the user to be visible to all users on the same post office as the user. Setting the visibility level to None means that no users will see the user in the Address Book. However, even if the user is not displayed in the Address Book, other users can send messages to the user by typing the user's ID (mailbox ID) in a message's To field.

   Account ID: This field supports accounting for GroupWise gateways. For more information about gateway accounting, see your gateway documentation.

   Expiration Date: Use this to set a date when the user's account will expire. The user will not be able to access the account after that date. For more information, see "Expiring a GroupWise Account" on page 217.

   Gateway Access: This is used to grant or restrict access to some GroupWise gateways. See your gateway documentation (http://www.novell.com/documentation/gw65/index.html) to determine if this field applies.

9. Modify information on any of the other tabs to configure the template, then click OK to save the template changes.

Creating a User Account from a Template

1. In ConsoleOne, right-click the container where you want to create a new eDirectory user, then click New > User.
2. Enter a Name, Surname, and Unique ID (all three are required).
3. Select the Use Template option, then browse to and select the template you want applied to this user.
4. Modify any of the other options you want.
5. Click OK to create the user's eDirectory and GroupWise accounts.

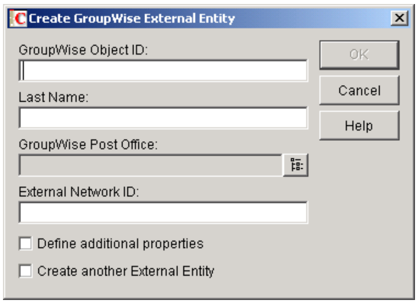
Creating GroupWise Accounts for Non-eDirectory Users

If you have users who do not have eDirectory accounts, you can still assign them GroupWise accounts by defining them as GroupWise external entities in eDirectory. Defining a user as a GroupWise external entity provides the user with access to GroupWise only; it does not enable the user to log in to eDirectory. External entities have eDirectory objects, but they are not considered eDirectory users for licensing purposes.

To create a GroupWise account for a non-eDirectory user:

1 In ConsoleOne, right-click the eDirectory container where you want to create the user's GroupWise External Entity object, then click New > Object to display the New Object dialog box.

2 Select GroupWise External Entity, then click OK to display the Create GroupWise External Entity dialog box.


Create GroupWise External Entity
GroupWise Object ID:
Last Name:
GroupWise Post Office:
External Network ID:
☐ Define additional properties
☐ Create another External Entity
OK
Cancel
Help

3 Fill in the following fields:

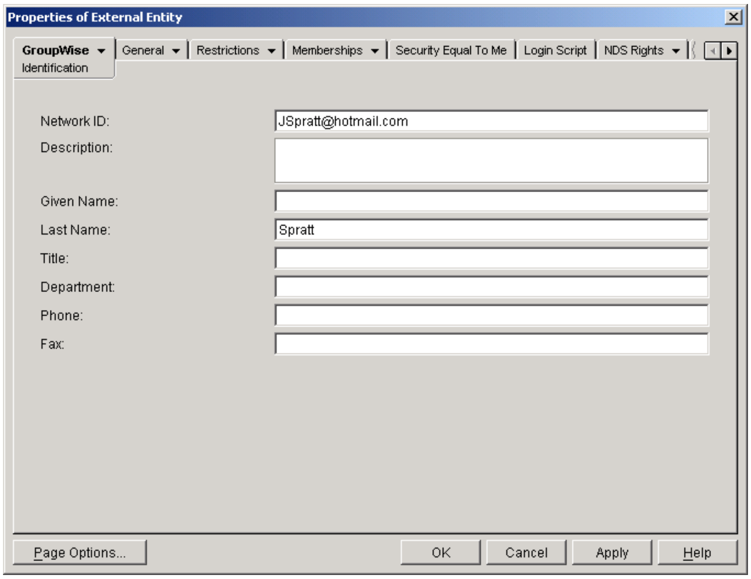
GroupWise Object ID: Enter the user's GroupWise ID. The user's ID along with the user's post office and domain, provide the user with a unique name within the GroupWise system (*userID.po.domain*). The GroupWise object ID cannot include periods.

Last Name: Enter the user's last name.

GroupWise Post Office: Select the post office where you want the user's mailbox.

External Network ID: Enter the user's network ID for the network that he or she logs in to.

4 Select Define Additional Properties, then click OK to display the GroupWise Identification page.



Network ID: JSpratt@hotmail.com

Last Name: Spratt

5 If desired, fill in any of the fields on the Identification page.

This information will appear in the GroupWise Address Book, as described in Chapter , "Address Book," on page 81. If you want to keep private information in the Description field, you can prevent this information from appearing the GroupWise Address Book. See "Preventing the User Description Field from Displaying in the Address Book" on page 85.

6 Click OK to save the information.

The user is given a GroupWise mailbox in the post office you selected and can access his or her mailbox through the GroupWise client.

Educating Your New Users

After users can log in to their GroupWise accounts, all of the GroupWise client's features are at their fingertips, but some new users do not know how to get started. You can give your users the following suggestions to encourage them to explore the GroupWise client:

- Click Help > Help Topics > Contents > How Do I to learn to perform common GroupWise tasks
- Click Help > What's New to learn about the latest new GroupWise features
- Click Help > User Guide to view the *GroupWise 6.5 Windows Client User Guide* in HTML format
- Print "Getting Started" in the *GroupWise 6.5 Windows Client User Guide* to keep handy by the workstation as a quick reference

For convenience in printing, the *GroupWise 6.5 Windows Client User Guide* is available in PDF format at the GroupWise 6.5 Documentation Web site (http://www.novell.com/documentation/gw65/index.html).

14 Managing GroupWise Accounts and Users

As your GroupWise® system grows, you will need to add users and manage their GroupWise accounts.

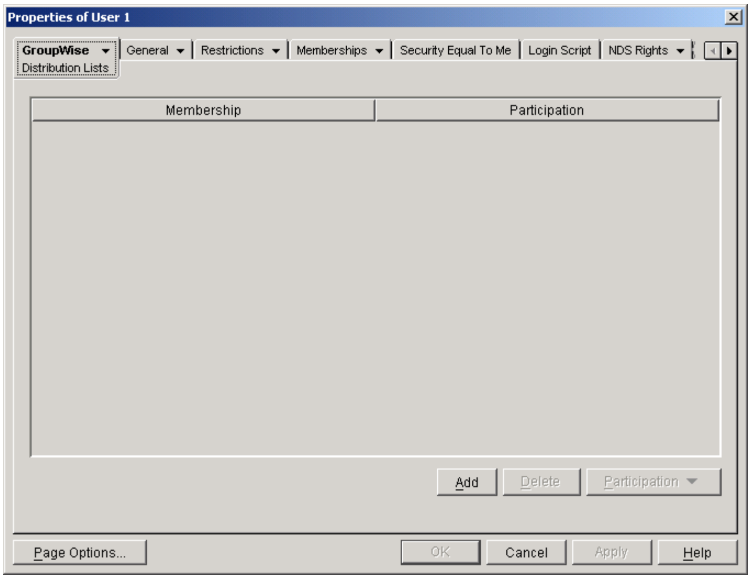
See also "Maintaining Domain and Post Office Databases" on page 345, Chapter 27, "Maintaining User/Resource and Message Databases," on page 353, and "Backing Up GroupWise Databases" on page 375. Proper database maintenance and backups allow recovery from accidental deletions, as described in "Restoring Deleted Mailbox Items" on page 381 and "Recovering Deleted GroupWise Accounts" on page 384.

Adding a User to a Distribution List

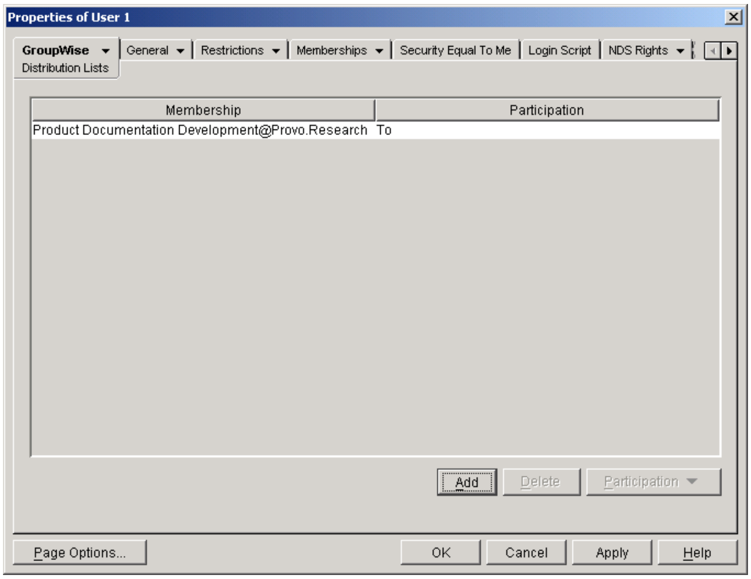
GroupWise® distribution lists are sets of users and resources that can be addressed as a single entity. When a GroupWise user addresses an item (message, appointment, task, or note) to a distribution list, each user or resource that is a member receives a copy of the item.

To add a user to a distribution list

1. In ConsoleOne, right-click the User object, then click Properties.
2. Click GroupWise > Distribution Lists to display the Distribution Lists page.



3 Click Add, select the distribution list that you want to add the user to, then click OK.



Membership	Participation
Product Documentation Development@Provo.Research	To

By default, the user is added as a primary recipient (To: recipient).

4 If you want to change the resource's recipient type, select the distribution list, click Participation, then click To, CC, or BC.

5 Click OK to save your changes.

Moving GroupWise Accounts

Expansion or consolidation of your GroupWise system can make it necessary for you to move GroupWise accounts from one post office to another.

When you move a GroupWise account, the user's mailbox is physically moved from one post office directory to another. The user's Novell® eDirectory™ object, including the GroupWise account information, remains in the same eDirectory container.

The following sections provide information you should know before performing a move and instructions to help you perform the move.

- "Live Move vs. File Transfer Move" on page 199
- "Moves Between GroupWise 6.x Post Offices" on page 199
- "Moves Between GroupWise 6.x and GroupWise 5.x Post Offices" on page 199
- "Preparing for a Move" on page 200
- "Moving a GroupWise Account to Another Post Office in the Same eDirectory Tree" on page 200
- "Moving a GroupWise Account to Another Post Office in a Different eDirectory Tree" on page 201
- "Monitoring User Move Status" on page 203

Live Move vs. File Transfer Move

GroupWise 6.*x* supports two types of moves: a live move and a file transfer move.

A live move uses a TCP/IP connection between Post Office Agents (POAs) to move a user from one post office to another. In general, a live move is significantly faster (approximately 5 to 10 times) than a file transfer move. However, it does require that both POAs are version 6.*x* and that TCP/IP is functioning efficiently between the two POAs. A file transfer move uses the transfer of message files (using POAs and MTAs) rather than a TCP/IP connection between POAs. A file transfer move is required if you are moving a user to a post office that is not using a GroupWise 6.*x* POA or if you are moving a user across a WAN link where TCP/IP might not be efficient.

By default, when you initiate a move from a GroupWise 6.*x* post office, the post office's POA attempts to establish a live move session with the destination post office's POA. If it cannot, a file transfer move is used instead.

If desired, you can disable the live move capability on a GroupWise 6.*x* post office (Post Office object > GroupWise tab > Identification page). Any moves to or from the post office would be done by file transfer.

Moves Between GroupWise 6.*x* Post Offices

When you move a user's account from one GroupWise 6.*x* post office to another, all items are moved correctly and all associations (proxy rights, shared folder access, and so forth) are resolved so that the move is transparent to the user. Occasionally, some client options the user has set (GroupWise client > Tools menu > Options) might be lost and must be re-created for the new mailbox.

Moves Between GroupWise 6.*x* and GroupWise 5.*x* Post Offices

Moves that include a GroupWise 5.*x* post office are performed at the level supported by the 5.*x* post office. This means that users might experience the following:

- Rules need to be re-created.
- Folders do not appear in the same order as in the original mailbox.
- The Address Book contains more than one Frequent Contacts list or system address books.

- Folders and personal address books shared with others will no longer be shared. They will need to be shared again.
- Shared folders and personal address books received from others will no longer be available. They will need to be shared again.
- Proxy rights to other mailboxes are lost. The rights will need to be reestablished.
- Folders' sort order and column settings are lost. They will need to be reset.
- Query folders no longer work. The query will need to be performed again.
- Replies (from other users) to items sent by the moved user before the user moved will be undeliverable.
- Messages sent to the moved user from Remote client users will be undeliverable until the Remote client users download the Address Book again.

Preparing for a Move

Consider the following before moving a user's GroupWise account:

- Make sure the POAs for the user's current post office and destination post office are running. Make sure the Message Transfer Agent (MTA) for the user's current domain and destination domain (if different) are running.
- A user who owns a resource cannot be moved. If the user owns a resource, reassign ownership of the resource to another user who is on the same post office as the resource. You can do this beforehand (see "Changing a Resource's Owner" on page 227) or when initiating the move.
- (Optional) To reduce the number of mailbox items that must be moved, consider asking the user to clean up his or her mailbox by deleting or archiving items.
- (Optional) Have the user exit GroupWise and GroupWise Notify before you initiate the move. When the move is initiated, the user's POA first creates an inventory list of all information in the user's mailbox. This inventory list is sent to the new post office's POA so that it can verify when all items have been received. If the user remains logged in, any changes to the mailbox (received items, sent items, and so forth) after the inventory list is created will not be moved to the user's new mailbox. After the move has been initiated, the user can log in to his or her new mailbox even if the move is not complete.

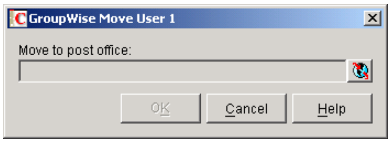
Moving a GroupWise Account to Another Post Office in the Same eDirectory Tree

The following steps apply only if the user's current post office and destination post office are located in the same eDirectory tree. If not, see "Moving a GroupWise Account to Another Post Office in a Different eDirectory Tree" on page 201.

To move a user's GroupWise account to a different post office in the same eDirectory tree:

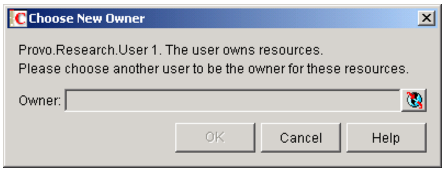
1. In ConsoleOne®, right-click the User object or GroupWise External Entity (in the GroupWise view) > click Move to display the GroupWise Move dialog box.

   If you want to move multiple users from the same post office to another post office, select all the User objects, right-click the selected objects > click Move.



2 Select the post office to which you want to move the user's account, then click OK.

If the user owns a resource, the following dialog box appears.



Provo.Research.User 1. The user owns resources.
Please choose another user to be the owner for these resources.

3 Select a new owner for the resource, then click OK.

4 Keep track of the user move process using the User Move utility. See "Monitoring User Move Status" on page 203

Resolving Addressing Issues Caused By Moving an Account

The user's new address information is immediately replicated to each post office throughout your system so that the system address book contains the user's updated address. Any user who selects the moved user from the system address book will be able to successfully send messages to the user.

However, some users might have the user's old address (GroupWise user ID) in their Address Book's Frequent Contacts list. In this case, if the sender types the moved user's name in the To field rather than selecting it from the system address book, GroupWise uses the old address stored in the Frequent Contacts list instead of the new address in the system address book. This will result in the message being undeliverable. The POA automatically resolves this issue when it performs its nightly user upkeep (see "Performing Nightly User Upkeep" on page 472). During the nightly user upkeep process, the POA ensures that all addresses in a user's Frequent Contacts list are valid addresses in the system address book.

If you want to ensure that messages sent to the user's old address are delivered even before the POA cleans up the Frequent Contacts List, you can create a nickname using the old GroupWise user ID. For information about creating a nickname, see "Creating a Nickname for a User" on page 213. To have a nickname created automatically when the user is moved, see "System Preferences" on page 44.

Moving a GroupWise Account to Another Post Office in a Different eDirectory Tree

A GroupWise system can span multiple eDirectory trees, provided that all components for a single domain (post offices, users, resources, and so forth) are all in the same eDirectory tree. For example, a user cannot be located in one tree and his or her post office in another.

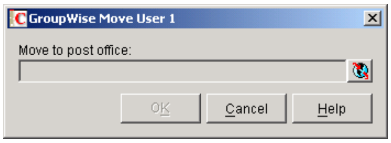
If necessary, you can move a user's account from a post office in one eDirectory tree to a post office in another eDirectory tree as long as the post offices are in the same GroupWise system. This requires the user to have a User object (or GroupWise External Entity object) in the eDirectory tree to which his or her GroupWise account is being moved.

To move a user's GroupWise account to a post office in a different eDirectory tree:

1 Make sure the user has a User object or GroupWise External Entity object in the eDirectory tree to which his or her GroupWise account is being moved.

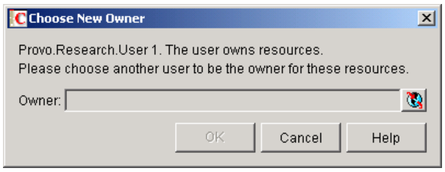
2 In ConsoleOne, right-click the User object or GroupWise External Entity object (in the GroupWise View) > click Move to display the GroupWise Move dialog box.

If you want to move multiple users from the same post office to another post office, select all the User objects, right-click the selected objects > click Move.



3 Select the post office to which you want to move the user's account, then click OK.

If the user owns a resource, the following dialog box appears.



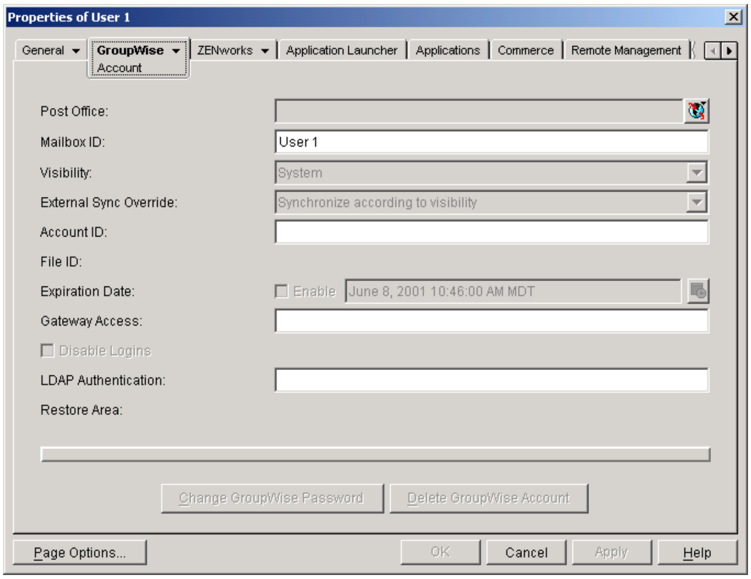
Provo.Research.User 1. The user owns resources.
Please choose another user to be the owner for these resources.

4 Select a new owner for the resource, then click OK.

5 Keep track of the user move process by using the User Move utility to determine when the user has been successfully moved. See "Monitoring User Move Status" on page 203

6 In the destination eDirectory tree, right-click the User object or GroupWise External Entity object where the GroupWise account will be assigned. This is the object referred to in Step 1.

7 Click GroupWise > Account to display the Account page.



Mailbox ID: User 1
Visibility: System
External Sync Override: Synchronize according to visibility
Expiration Date: □ Enable June 8, 2001 10:46:00 AM MDT

8 In the Post Office field, select the post office that the user's GroupWise account was moved to.

9. In the Mailbox ID field, make sure that the mailbox ID is the same as the user's mailbox ID (GroupWise user ID) on his or her original post office.

10. Click OK.

    A dialog box appears asking if you want to match the GroupWise account to this eDirectory user.

11. Click Yes.

Resolving Addressing Issues Caused By Moving an Account

The user's new address information is immediately replicated to each post office throughout your system so that the system address book contains the user's updated address. Any user who selects the moved user from the system address book will be able to successfully send messages to the user.

However, some users might have the moved user's old address (GroupWise user ID) in their Address Book's Frequent Contacts list. In this case, if the sender types the moved user's name in the To field instead of selecting it from the system address book, GroupWise uses the old address stored in the Frequent Contacts list instead of the new address in the system address book. This will result in the message being undeliverable. The POA automatically resolves this issue when it performs its nightly user upkeep (see "Performing Nightly User Upkeep" on page 472). During the nightly user upkeep process, the POA ensures that all addresses in a user's Frequent Contacts list are valid addresses in the system address book.

If you want to ensure that messages sent to the user's old address are delivered even before the POA cleans up the Frequent Contacts List, you can create a nickname using the old GroupWise user ID. For information about creating a nickname, see "Creating a Nickname for a User" on page 213. To have a nickname created automatically when the user is moved, see "System Preferences" on page 44.

Monitoring User Move Status

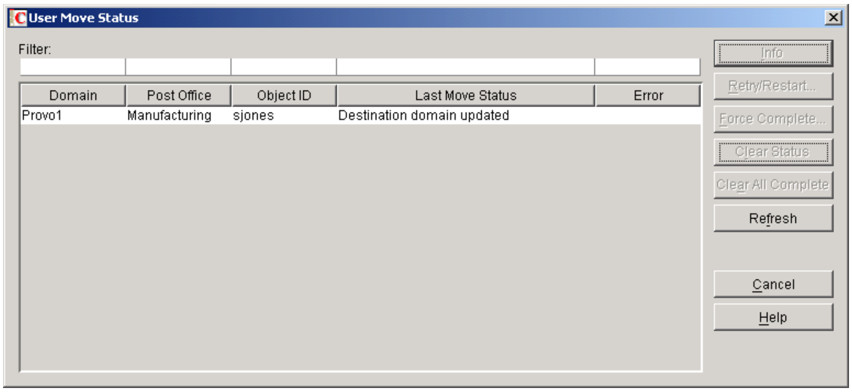
The User Move Status utility helps you track progress as you move users and resources from one post office to another. It displays the user moves associated with the object you selected before displaying the User Move Status dialog box. For example, if you selected a Domain object, all user moves for the selected domain are displayed, but not user moves for other domains.

While a GroupWise user account is being moved, the POA in the source post office and the POA in the destination post office communicate back and forth. You can track the move process progresses through various steps and statuses:

1. In ConsoleOne, select a Post Office or Domain object.

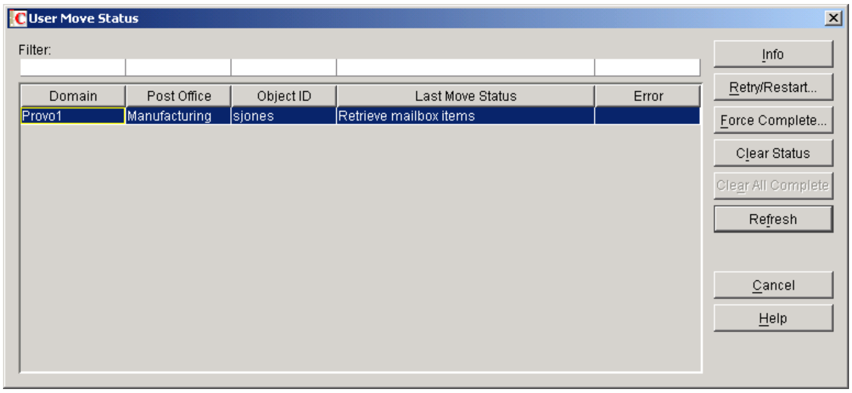
   All moves occurring within the selected location will be listed.

2. Click Tools > GroupWise Utilities > User Move Status.



Domain	Post Office	Object ID	Last Move Status	Error
Provo1	Manufacturing	sjones	Destination domain updated	

At the beginning of the move process, most button are dim, because it would not be safe for you to perform those actions at that point in the move process. When those actions become safe, the buttons become active.



Domain	Post Office	Object ID	Last Move Status	Error
Provo1	Manufacturing	sjones	Retrieve mailbox items	

3 To restrict the number of users and resources in the list, type distinguishing information in any of the Filter fields, then press Enter to filter the list.

4 During the move, click Refresh to update the status information.

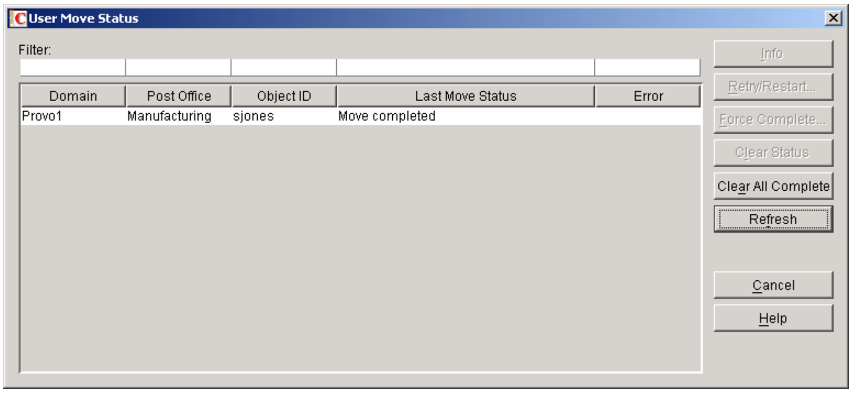
IMPORTANT: The list does not refresh automatically.

During the move, you might observe some of the following statuses:

- **Destination post office updated:** The destination POA has updated the destination post office database with the user's account information. At this point, the user account exists in the new location and appears in the Address Book with the new location information.
- **Source post office updated:** The source POA has removed the user from the source post office database. At this point, the user can no longer access the mailbox at the old location.
- **Moving mailbox information:** The POAs have finished exchanging administrative information and are ready to move items from the old mailbox to the new mailbox.
- **Sending mailbox inventory list:** The source POA sends the destination POA a list of all the mailbox items that it should expect to receive.
- **Send item request:** The destination POA starts requesting items from the source POA and the source POA responds to the requests
- **Retry mailbox item retrieval:** The destination POA was unable to retrieve an item and is retrying. The POA continues to retry every 12 hours for 7 days, then considers the

move complete. To complete the move without waiting, click Force Complete. Typically, items that cannot be moved were not accessible to the user in the first place, so nothing is missed in the destination mailbox.

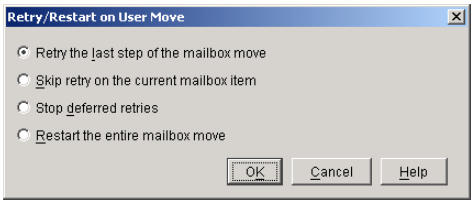
- **Completed retrieving items:** The destination POA has received all of the items on its mailbox inventory list.
- **Move completed:** After all of the user's mailbox items have arrived in the destination post office, the user's original account in the source post office is deleted and the user move is finished.



Domain	Post Office	Object ID	Last Move Status	Error
Provo1	Manufacturing	sjones	Move completed	

The User Move Status utility cannot gather status information for destination post offices that are running POAs older than GroupWise 6.5. Status information for users moving to older post offices displays as Unavailable.

5 If something disrupts the user move process, select the problem user or resource, then click Retry/Restart.



● Retry the last step of the mailbox move
○ Skip retry on the current mailbox item
○ Stop deferred retries
○ Restart the entire mailbox move

6 Select the option appropriate to the problem you are having, then click OK.

Retry the Last Step of the Mailbox Move: Select this option to retry whatever step the user move process has stopped on. This is equivalent to performing one of the POA's automatic retries manually and immediately. Ideally, the step will complete successfully on the retry and processing will continue normally.

Skip Retry on the Current Mailbox Item: Select this option to skip a particular mailbox item that cannot be successfully moved. The need for this action can usually be avoided by running Mailbox/Library Maintenance on the mailbox before moving the user account. Ideally, the user move processing should continue normally after skipping the problem item.

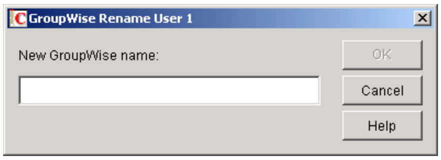
Stop Deferred Retries: Select this option to stop the POA from retrying to send items that have not been successfully received. This completes the user move process even though some individual items have not been moved successfully.

Restart the Entire Mailbox Move: Select this option if something major disrupts the user move process and you want to start over from the beginning. Because nothing is deleted from the source mailbox until everything has been received in the destination mailbox, you can safely restart a move at any time for any reason.

Renaming Users and Their GroupWise Accounts

When you rename a user, the user's GroupWise user ID (mailbox ID) changes but the user remains in the same post office. All of the user's associations remain unchanged. For example, the user retains ownership of any documents and resources while other users who had proxy rights to the user's mailbox retain proxy right.

1. Make sure the user has exited GroupWise and GroupWise Notify.
2. Make sure the domain's MTA and post office's POA are running.
3. In the GroupWise View, right-click the User object > click Rename to display the GroupWise Rename dialog box.



4. Enter the GroupWise user ID.
5. Click OK to rename the user.

Resolving Addressing Issues Caused By Renaming a User

The user's new information is immediately replicated to each post office throughout your system so that the system address book contains the user's updated address. Any user who selects the renamed user from the system address book will be able to successfully send messages to the renamed user.

However, some users might have the user's old address (GroupWise user ID) in their Address Book's Frequent Contacts List. In this case, if the sender types the renamed user's name in the To field instead of selecting it from the system address book, GroupWise uses the old address stored in the Frequent Contacts List instead of the new address in the system address book. This will result in the message being undeliverable. The POA automatically resolves this issue when it performs its nightly user upkeep (see "Performing Nightly User Upkeep" on page 472). During the nightly user upkeep process, the POA ensures that all addresses in a user's Frequent Contacts List are valid addresses in the system address book.

If you want to ensure that messages sent to the user's old address are delivered even before the POA cleans up the Frequent Contacts List, you can create a nickname using the old GroupWise user ID. For information about creating a nickname, see "Creating a Nickname for a User" on page 213.

Managing Mailbox Passwords

The following sections provide information to help you manage GroupWise mailbox passwords:

- "Creating or Changing a Mailbox Password" on page 207
- "Removing a Mailbox Password" on page 208
- "Bypassing the GroupWise Password" on page 208

For background information about GroupWise passwords, see Chapter 79, "GroupWise Passwords," on page 1033.

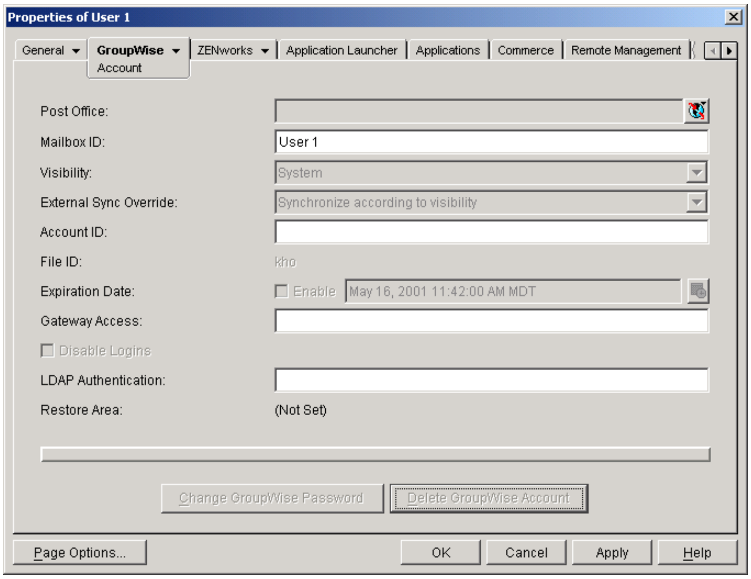
Creating or Changing a Mailbox Password

As administrator, you can use ConsoleOne to create a user's mailbox password or change a user's existing password. If a user can log in to GroupWise, he or she can also change the mailbox password through the Security Options dialog box (GroupWise Windows client > Tools menu > Options > Security) or on the Passwords page (GroupWise WebAccess client > Options > Password.

To create or change a user's mailbox password:

1 In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click Properties.

2 Click GroupWise > Account to display the Account page.



Post Office:

Mailbox ID: User 1

Visibility: System

External Sync Override: Synchronize according to visibility

Account ID:

File ID: kho

Expiration Date: □ Enable May 16, 2001 11:42:00 AM MDT

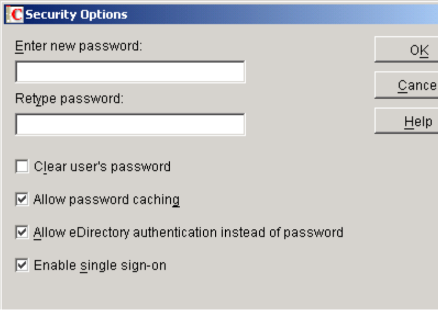
Gateway Access:

□ Disable Logins

LDAP Authentication:

Restore Area: (Not Set)

3 Click Change GroupWise Password to display the Security Options dialog box.



Enter new password:

Retype password:

□ Clear user's password

☑ Allow password caching

☑ Allow eDirectory authentication instead of password

☑ Enable single sign-on

4 Enter and reenter a new password.

The other options in this dialog box are explained in following sections.

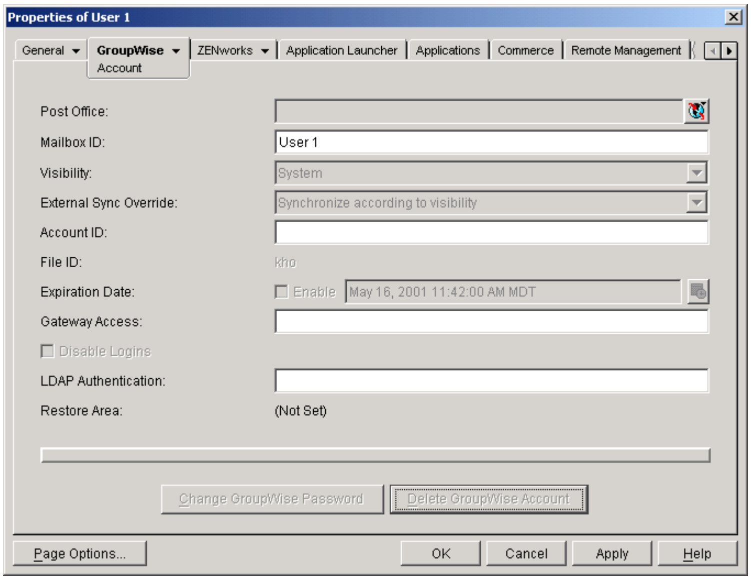
5 Click OK.

Removing a Mailbox Password

If you want to remove a user's mailbox password but not assign a new password, you can clear the password.

1 In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click Properties.

2 Click GroupWise > Account to display the Account page.



Post Office:

Mailbox ID: User 1

Visibility: System

External Sync Override: Synchronize according to visibility

Account ID:

File ID: kho

Expiration Date: □ Enable May 16, 2001 11:42:00 AM MDT

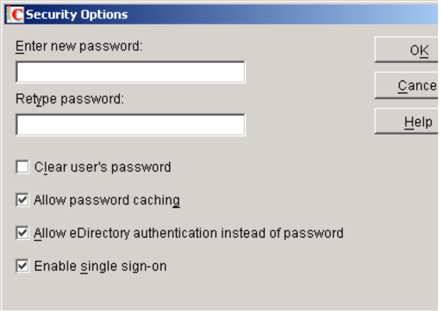
Gateway Access:

□ Disable Logins

LDAP Authentication:

Restore Area: (Not Set)

3 Click Change GroupWise Password to display the Security Options dialog box.



Enter new password:

Retype password:

□ Clear user's password

☑ Allow password caching

☑ Allow eDirectory authentication instead of password

☑ Enable single sign-on

4 Select the Clear User's Password option.

The other options in this dialog box are explained in following sections.

5 Click OK.

Bypassing the GroupWise Password

By default, if a user must enter a password when logging in to GroupWise, he or she is prompted for the password.

The GroupWise client includes several options that users can choose from to enable them to log in without providing a password. These options, located on the Security Options dialog box (GroupWise client > Tools menu > Options > Security), are described in the following table.

GroupWise Client Option	Description
Remember My Password	This option is available only when running the GroupWise client on Windows 95/98. The GroupWise password is stored in the Windows password list. When GroupWise starts, it pulls the password from the list.
No Password Required with eDirectory	This option is available only when logged in to Novell eDirectory. When GroupWise starts, it automatically logs in to the GroupWise account associated with the user who is logged in to eDirectory at the workstation. No GroupWise password is required.
Use Novell Single Sign-On	This option is available only when using the Novell Single Sign-on product. When GroupWise starts, it uses the GroupWise password stored by Novell Single Sign-on.

As shown in the table, these options will appear only if certain conditions are met, such as the user running on a Windows 95/98 workstation or having Novell Single Sign-on installed. If you don't want the option available to users even if the condition is met, you can disable the option. Doing so removes it from the GroupWise client's Password dialog box.

To disable one or more of the password options:

1 In ConsoleOne, click a Domain object if you want to disable password options for all users in the domain.

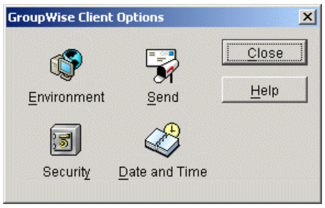
or

Click a Post Office object if you want to disable password options for all users in the post office.

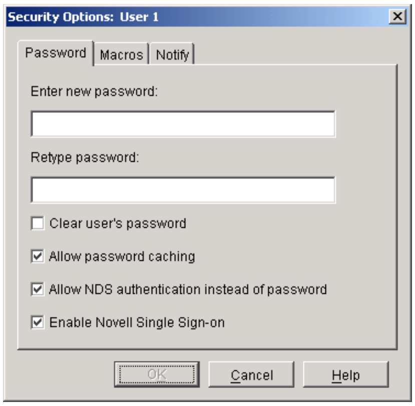
or

Click a User object or GroupWise External Entity object if you want to disable password options for the individual user.

2 With the appropriate GroupWise object selected, click Tools menu > GroupWise Utilities > Client Options to display the GroupWise Client Options dialog box.



3 Click Security to display the Security Options dialog box.



Enter new password:

Retype password:

□ Clear user's password

☑ Allow password caching

☑ Allow NDS authentication instead of password

☑ Enable Novell Single Sign-on

4. On the Password tab, deselect Allow Password Caching if you don't want Windows 95/98 users to be able to use the GroupWise client's Remember My Password option.
5. Deselect Allow eDirectory Authentication Instead of Password if you don't want eDirectory users to be able to use the GroupWise client's No Password Required with eDirectory option.
6. Deselect Allow Novell Single Sign-on if you don't want Single Sign-on users to be able to use the GroupWise client's Use Novell Single Sign-on option.
7. Click OK to save your changes.

For more information about addressing formats, see Chapter , "Internet-Style Addressing," on page 87.

Managing E-Mail Addresses

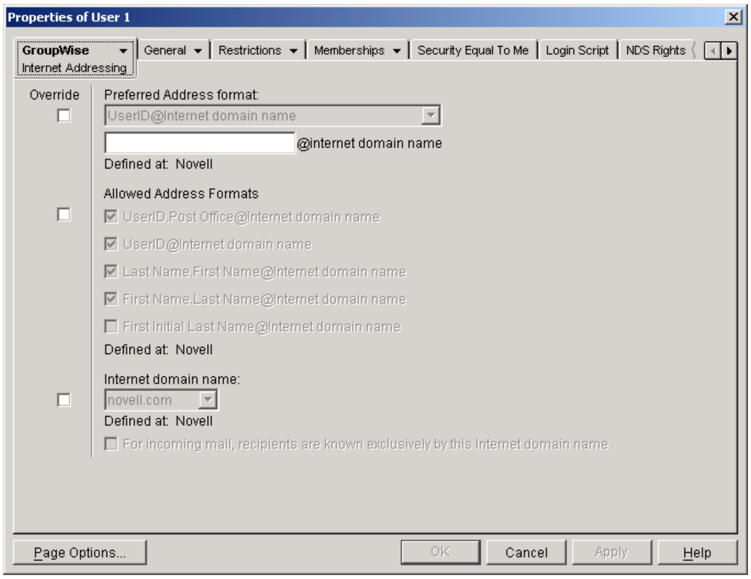
To ensure that user addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for users. The following sections provide details:

- "Changing a User's Internet Addressing Settings" on page 210
- "Changing a User's Visibility in the Address Book" on page 212
- "Creating a Nickname for a User" on page 213

Changing a User's Internet Addressing Settings

By default, a user inherits his or her Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from the user's post office, domain, or GroupWise system. If necessary, you can override these settings for individual users.

1. In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click Properties.
2. Click GroupWise > Internet Addressing to display the Internet Addressing page.



Override

□ Preferred Address format: UserID@Internet domain name

@internet domain name

Defined at: Novell

Allowed Address Formats

□

☑ UserID.Post Office@Internet domain name

☑ UserID@Internet domain name

☑ Last Name.First Name@Internet domain name

☑ First Name.Last Name@Internet domain name

☐ First Initial Last Name@Internet domain name

Defined at: Novell

Internet domain name:

□ novell.com

Defined at: Novell

☐ For incoming mail, recipients are known exclusively by this Internet domain name

3 To override one of the settings, select the Override box, then change the setting.

Preferred Address Format: The preferred address format determines how the user's address will be displayed in the GroupWise Address Book and in sent messages.

At the user and resource level, the preferred address format can be completely overridden by explicitly defining the user portion of the address format (*user@Internet domain name*). The user portion can include any RFC-compliant characters (no spaces, commas, and so forth).

For example, if you've selected *First Name.Last Name@Internet domain name* as your system's preferred address format and you have two John Petersons, each on a different post office in your system, you would end up two users having the same address (John.Peterson@novell.com). You could use this field to differentiate them by including their middle initials in their addresses (John.S.Peterson@novell.com and John.A.Peterson@novell.com).

Allowed Address Formats: The allowed address formats determine which address formats can be used to send messages to the user. For example, using John Peterson as the user, Research as the post office, and novell.com as the Internet domain, if you select all five formats, John Peterson would receive messages sent using any of the following addresses:

jpeterson.research@novell.com
jpeterson@novell.com
john.peterson@novell.com
peterson.john@novell.com
jpeterson@novell.com

Internet Domain Name: The Internet domain name, along with the preferred address format, is used when constructing the e-mail address that is displayed in the GroupWise Address Book and in the To field of sent messages.

Only the Internet domain names that have been defined are displayed in the list. Internet domain names must be defined at the system level (Tools menu > GroupWise System Operations > Internet Addressing). For more information, see "Internet-Style Addressing" on page 87.

If you override the Internet domain name, the For Incoming Mail, Recipients are Known Exclusively by This Internet Domain Name becomes available. Enable this option if you only want the user to be able to receive messages addressed with this Internet domain name. If you don't enable this option, the user will receive messages addressed using any of the Internet domain names assigned to your GroupWise system.

4 Click OK to save your changes.

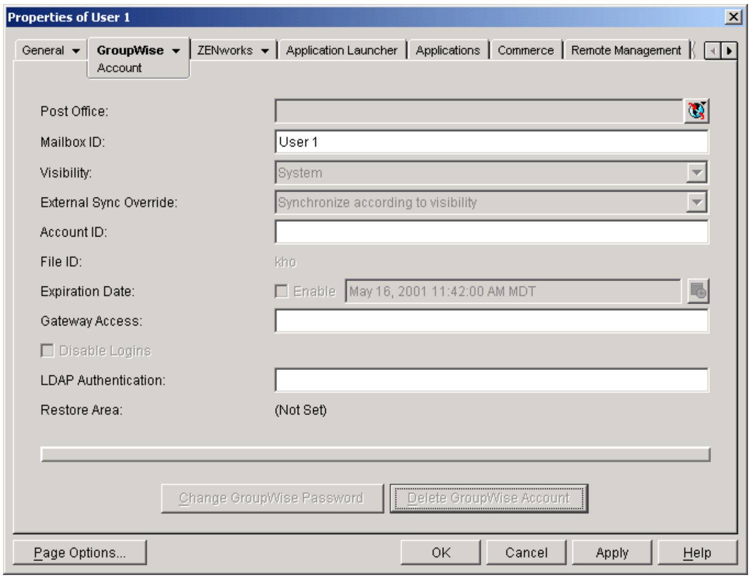
Changing a User's Visibility in the Address Book

A user's visibility level determines the extent to which the user's address is visible throughout your GroupWise system. You can make the user visible in the Address Book throughout your entire GroupWise system, you can limit visibility to the user's domain or post office only, or you can make it so that no users can see the user in the Address Book.

Making a user visible in the Address Book simply makes it easier to address items to the user. However, regardless of a user's visibility, other users can send items to the user if they know the user's GroupWise user ID.

1 In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click Properties.

2 Click GroupWise > Account to display the Account page.



Post Office:

Mailbox ID: User 1

Visibility: System

External Sync Override: Synchronize according to visibility

Account ID:

File ID: kho

Expiration Date: □ Enable May 16, 2001 11:42:00 AM MDT

Gateway Access:

□ Disable Logins

LDAP Authentication:

Restore Area: (Not Set)

3 In the Visibility field, select the desired visibility level.

System (Default): All users in your GroupWise system will be able to see the user's information in the Address Book.

Domain: Only users in the same domain as the user will be able to see the user's information in the Address Book.

Post Office: Only users in the same post office as the user will be able to see the user's information in the Address Book.

None: No users will be able to see the user's information in the Address Book. Users will need to know the user's GroupWise user ID to send items to him or her.

4 Click OK to save your changes.

Creating a Nickname for a User

Each user has a specific GroupWise address consisting of the user's ID, post office, and domain (*user_ID.post_office.domain*). You can assign one or more nicknames to a user to give the user an alternate address. Each part of the address (*user_ID*, *post_office*, and *domain*) can be different than the user's actual address.

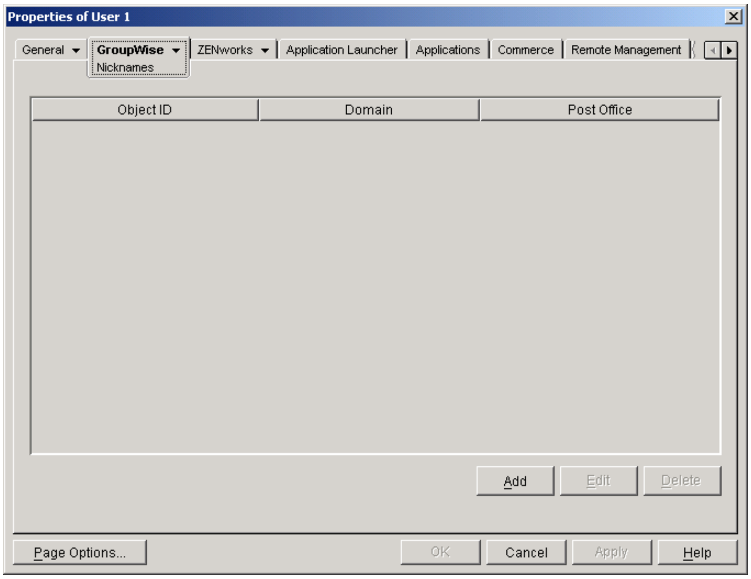
For example, you might want to create a nickname for a user you have just moved (see "Moving GroupWise Accounts" on page 198) or renamed (see "Renaming Users and Their GroupWise Accounts" on page 206). The nickname, which would be the user's old address, would ensure that any use of the old address would result in the new address being used instead.

Nicknames are not displayed in the Address Book, which means users will need to know the nickname to use it.

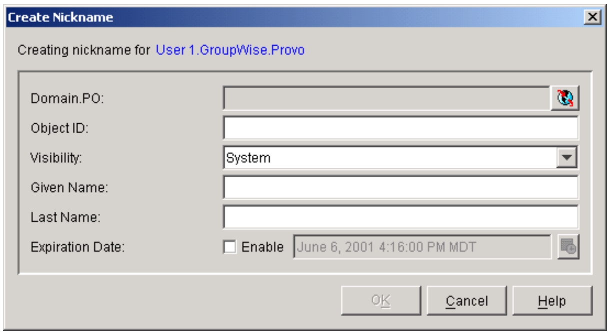
To manually create a nickname for a user:

1 In ConsoleOne, right-click the User object or GroupWise External Entity object, then click Properties.

2 Click GroupWise > Nicknames to display the Nicknames page.



3 Click Add to display the Create Nickname dialog box.



Creating nickname for User 1.GroupWise.Provo

Domain.PO:

Object ID:

Visibility: System

Given Name:

Last Name:

Expiration Date: □ Enable June 6, 2001 4:16:00 PM MDT

4 Fill in the following fields:

Domain.PO: Select the post office where you want to assign the nickname. This can be any post office in your GroupWise system; it does not have to be the user's post office.

Object ID: Enter the name to use as the *user_ID* portion of the nickname. The nickname must be unique.

Visibility: This field does not apply to nicknames. Nicknames are not displayed in the Address Book. To use a nickname, a message sender must enter the nickname's address.

Given Name: Enter the user's given (first) name.

Last Name: Enter the user's last name.

Expiration Date: If you want the nickname to no longer work after a certain date, click Enable and then select the desired date.

5. Click OK to add the nickname to the list.
6. Click OK to save the changes to the User object or GroupWise External Entity object.

To have nicknames created automatically whenever you move a user, see "System Preferences" on page 44.

Checking GroupWise Account Usage

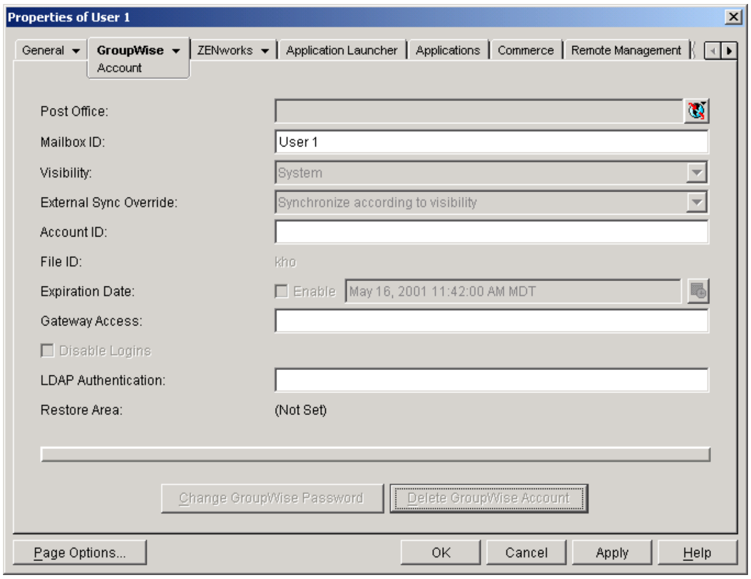
You can identify GroupWise accounts that have been inactive for a specified period of time. See "Auditing Mailbox License Usage in the Post Office" on page 180.

You can measure message traffic from individual GroupWise mailboxes. See "User Traffic Report" on page 933.

Disabling and Enabling GroupWise Accounts

You can disable a GroupWise account so that the user cannot access his or her mailbox until you enable the account again. This might be necessary if you need to perform database maintenance on the user's mailbox or when a user leaves the company and no longer needs access to the mailbox.

1. In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click Properties.
2. Click GroupWise > Account to display the Account page.



Post Office:
Mailbox ID: User 1
Visibility: System
External Sync Override: Synchronize according to visibility
Account ID:
File ID: kho
Expiration Date: □ Enable May 16, 2001 11:42:00 AM MDT
Gateway Access:
□ Disable Logins
LDAP Authentication:
Restore Area: (Not Set)

3 Select Disable Logins, then click OK.

4 To enable the user’s account when access is again permitted, deselect Disable Logins, then click OK.

While a user’s account is disabled, other users to whom proxy rights have been granted can still access the mailbox. This is convenient for reviewing the contents of the mailbox of a departed employee and pulling out those messages that are of use to the incoming employee.

Removing GroupWise Accounts

You can remove a user’s GroupWise account by deleting or expiring it. Deleting an account removes the entire account (address, mailbox, items, and so forth) from the GroupWise system. Expiring an account deactivates the account so that it cannot be accessed, but does not remove if from the system. The following sections provide information to help you delete or expire GroupWise accounts

- “Deleting a GroupWise Account” on page 215
- “Expiring a GroupWise Account” on page 217
- “Managing Expired or Expiring GroupWise Accounts” on page 218

If you delete a GroupWise account by accident, or need to retrieve a deleted account for some other reason, see “Recovering Deleted GroupWise Accounts” on page 384.

NOTE: When you remove a GroupWise account, any personal databases, such as an archive, a Caching mailbox, or a Remote mailbox, that are associated with the account are unaffected by the account deletion. Such databases are not located where ConsoleOne could delete them, so they must be deleted manually.

Deleting a GroupWise Account

When you delete a user’s GroupWise account, the user’s mailbox is deleted and the user is removed from the GroupWise system. If the user owns library documents, see “Ensuring that a User’s Library Documents Remain Accessible” on page 216 before deleting the user. Otherwise, refer to one of the following sections:

- “Deleting an eDirectory User’s GroupWise Account” on page 216
- “Deleting a Non-eDirectory User’s GroupWise Account” on page 217

Ensuring that a User’s Library Documents Remain Accessible

When you delete a user’s GroupWise account, GroupWise does not delete any library documents to which the user has Author or Creator status. These documents remain in the library as "orphaned" documents, meaning that no one can access the documents.

If you or other users need access to the documents, you have the following choices:

- Rather than deleting the user, change the user’s GroupWise mailbox password so that he or she can’t log in. Other users will be able to continue accessing the documents, and you can log in as the user to manage the documents. For information about changing a user’s password, see “Creating or Changing a Mailbox Password” on page 207.
- Rather than deleting the user or changing the user’s password, disable the user’s ability to log in. This is done on the user’s GroupWise Account page (User object > GroupWise tab > Accounts page > Disable Logins).
- Delete the user, then reassign the orphaned documents to another user. For information, see “Analyzing and Fixing Library and Document Information” on page 360.

Deleting an eDirectory User’s GroupWise Account

1 Make sure the user has exited GroupWise and GroupWise Notify.

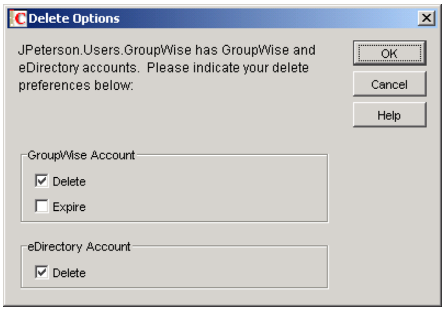
2 Make sure the POA (for the user’s post office) is running. If the POA is not running, the user’s mailbox will not be deleted until the next time the POA runs.

3 In ConsoleOne, right-click the User object, then click Delete.

or

Select multiple User objects, right-click the selected object, then click Delete.

4 Click Yes to display the Delete User Options dialog box.



JPeterson.Users.GroupWise has GroupWise and eDirectory accounts. Please indicate your delete preferences below:

GroupWise Account
☑ Delete
□ Expire

eDirectory Account
☑ Delete

5 In the GroupWise Account box, select Delete.

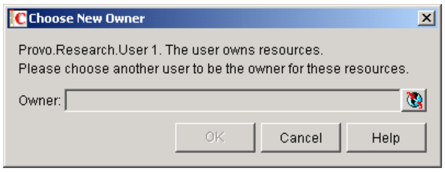
6 In the eDirectory Account box, deselect Delete.

7 Click OK to delete the eDirectory user’s GroupWise account.

or

If you selected multiple User objects, click OK to All to apply the same deletion options to all accounts. If you click OK rather than OK to All, you can select deletion options for each account individually as it is deleted.

8 If a user was a resource owner, the following dialog box appears. Select a new user to be the resource’s owner, then click OK.



Provo.Research.User1. The user owns resources.
Please choose another user to be the owner for these resources.

Owner:

Deleting a Non-eDirectory User’s GroupWise Account

Non-eDirectory users are given GroupWise accounts by adding the users to eDirectory as GroupWise external entities (see “Creating GroupWise Accounts for Non-eDirectory Users” on page 195). You remove a non-eDirectory user’s GroupWise account by deleting the user’s GroupWise External Entity object from eDirectory. (Remember that external entities do have eDirectory objects, but they are not considered eDirectory users for licensing purposes.)

As with eDirectory users, when you remove a non-eDirectory user’s GroupWise account, the user’s mailbox is deleted and the user is removed from the GroupWise system.

To delete a non-eDirectory user’s GroupWise account:

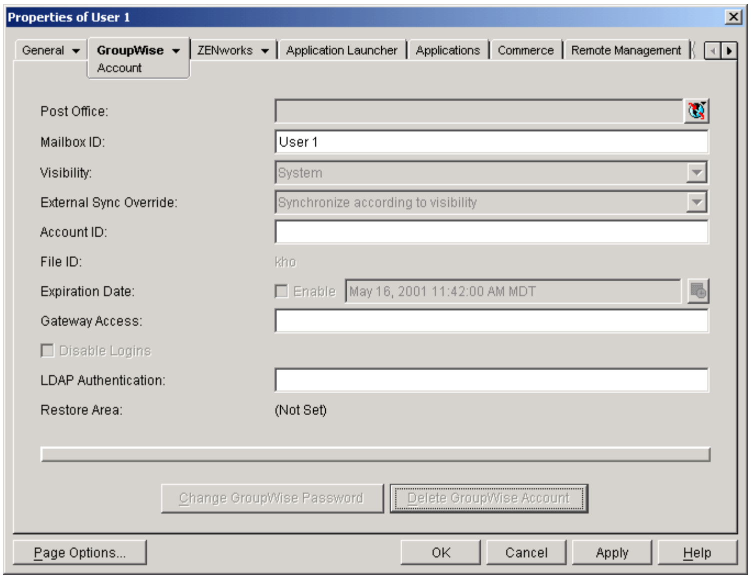
1. Make sure the user has exited GroupWise and GroupWise Notify.
2. Make sure the POA (for the user’s post office) is running. If the POA is not running, the user’s mailbox will not be deleted until the next time the POA runs.
3. In ConsoleOne, right-click the user’s GroupWise External Entity object, then click Delete.
4. Click Yes to confirm the deletion.

Expiring a GroupWise Account

Rather than delete a user’s GroupWise account, you can expire the account. The account, including the user’s mailbox and all items, remains in GroupWise but cannot be accessed by the user. If necessary, the user’s account can be reactivated at a later date (see “Managing Expired or Expiring GroupWise Accounts” on page 218). This option is useful for providing GroupWise accounts to temporary or contract employees who come and go.

You can set a user’s GroupWise account to expire immediately or at a future date and time.

1. Make sure the user has exited GroupWise and GroupWise Notify.
2. In ConsoleOne, right-click the User object or GroupWise External Entity object with the account you want to expire, then click Properties.
3. Click GroupWise > Account to display the Account page.



Post Office:

Mailbox ID: User 1

Visibility: System

External Sync Override: Synchronize according to visibility

Account ID:

File ID: kho

Expiration Date: □ Enable May 16, 2001 11:42:00 AM MDT

Gateway Access:

□ Disable Logins

LDAP Authentication:

Restore Area: (Not Set)

4 In the Expiration Date field, select the Enable check box to turn on the option.

5 If you want the account to expire immediately, leave the date and time set to the current date and time.

or

If you want the account to expire at a later date, select the desired date and time.

6 Click OK.

NOTE: To immediately expire an account assigned to an eDirectory user, you can also right-click the User object, click Delete, select the Expire GroupWise Account option, then click OK. This method is not available for non-eDirectory (GroupWise External Entity) users.

Managing Expired or Expiring GroupWise Accounts

Expired GroupWise accounts remain expired until you reactivate them or delete them. Refer to the following sections for information to help you manage expired accounts:

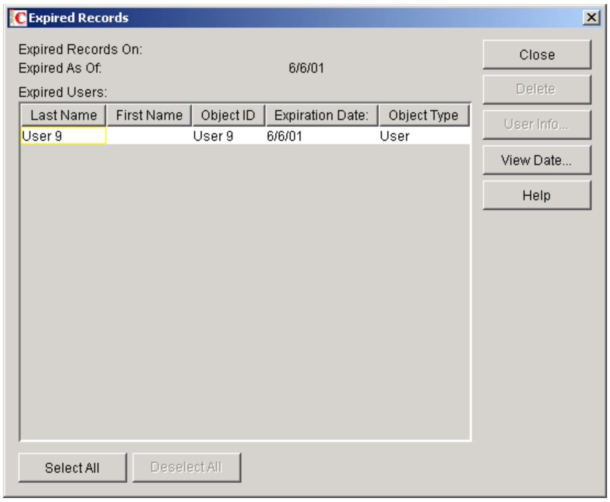
- "Identifying Expired or Expiring Accounts" on page 218
- "Changing an Account's Expiration Date" on page 219
- "Reactivating an Expired Account" on page 220

Identifying Expired or Expiring Accounts

Rather than search through all your User or GroupWise External Entity objects in eDirectory to identify which ones have expired or expiring accounts, you can use the Expired Records option to quickly list expired accounts for your entire system, a single domain, or a single post office. Depending on the date you choose, you can see expired accounts only or both expired and expiring accounts.

1 In the GroupWise View, select the post office, domain, or GroupWise system that contains the accounts you want to view.

2 Click Tools > GroupWise Utilities > Expired Records to display the Expired Records dialog box.



Expired Records On:
Expired As Of: 6/6/01
Expired Users:

Last Name	First Name	Object ID	Expiration Date:	Object Type
User 9		User 9	6/6/01	User

The Expired As Of field defaults to the current date. Only accounts that have expired as of this date are displayed in the list. To see accounts that will expire in the future, you need to change the date in the Expired As Of field.

3 To change the date in the Expired As Of field, click View Date, enter the desired date, then click OK.

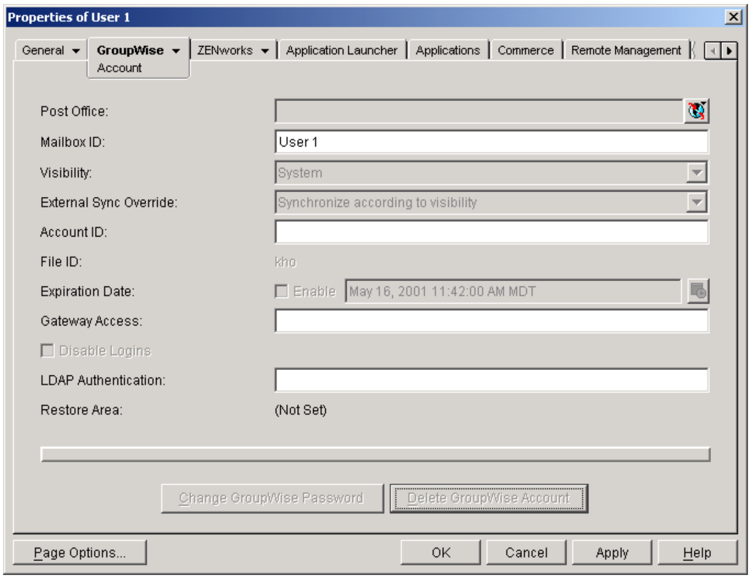
For example, in the dialog box shown above, the current date is 6/6/01 (June 6, 2001). To see what accounts will expire by June 30, 2001, you would change the Expired As Of date to 6/30/01.

4 When finished viewing expired or expiring accounts, click OK to close the Expired Accounts dialog box.

Changing an Account's Expiration Date

1 In ConsoleOne, right-click the User object or GroupWise External Entity object, then click Properties.

2 Click GroupWise > click Account to display the Account page.



Post Office:
Mailbox ID: User 1
Visibility: System
External Sync Override: Synchronize according to visibility
Account ID:
File ID: kho
Expiration Date: □ Enable May 16, 2001 11:42:00 AM MDT
Gateway Access:
□ Disable Logins
LDAP Authentication:
Restore Area: (Not Set)

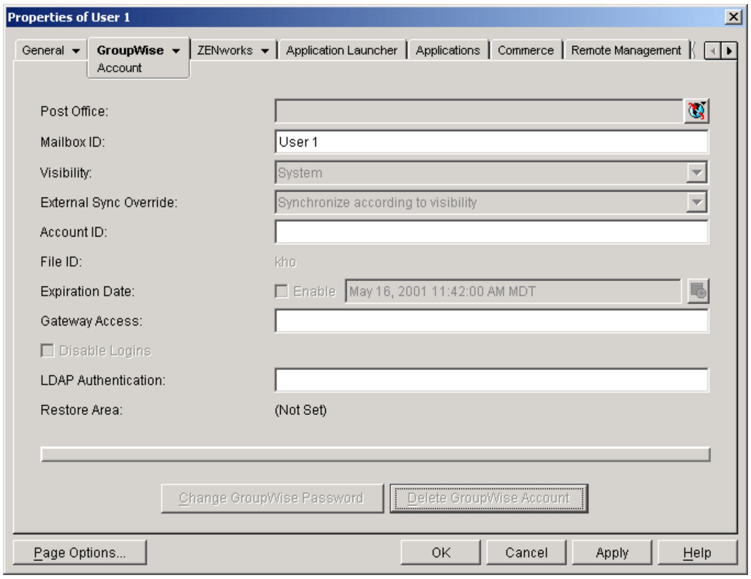
3 In the Expiration Date field, change the time and date.

4 Click OK.

Reactivating an Expired Account

1 In ConsoleOne, right-click the User object or GroupWise External Entity object with the expired GroupWise account, then click Properties.

2 Click GroupWise > Account to display the Account page.



Post Office:

Mailbox ID: User 1

Visibility: System

External Sync Override: Synchronize according to visibility

Account ID:

File ID: kho

Expiration Date: □ Enable May 16, 2001 11:42:00 AM MDT

Gateway Access:

□ Disable Logins

LDAP Authentication:

Restore Area: (Not Set)

3 In the Expiration Date field, deselect the Enable check box to turn off the option.

4 Click OK.

V Resources

15 Creating Resources

A resource is an item or place, such as a computer, company vehicle, or conference room, that users can schedule or check out.

- "Understanding Resources" on page 223
- "Planning Resources" on page 224
- "Creating a New Resource" on page 224

Understanding Resources

The following sections provide information to help you learn about GroupWise® resources:

- "Resource Objects" on page 223
- "Resource Types" on page 223
- "Resource Mailboxes" on page 223
- "Resource Owners" on page 224

Resource Objects

Each resource you want to make available must be added as a Resource object in Novell® eDirectory™. The name that you give the Resource object becomes the name by which the resource is displayed in the GroupWise Address Book.

Resource objects can be located in any eDirectory container that is in the same tree as the resource's domain.

Resource Types

You can identify the resource as a general resource or as a place. When a user schedules a resource that is defined as a place, the resource description is automatically added to the Place field in the appointment.

Resource Mailboxes

Like a user, a resource must be assigned to a post office so that it can be given an account (address, mailbox, and so forth). You assign the resource to a post office when you create the Resource object.

A resource's account enables it to receive scheduling requests (sent as appointments). The owner assigned to the resource can go into the resource's mailbox to accept or decline the requests. For example, you might want to have all your conference rooms defined as resources. When sending a meeting appointment, users could schedule the conference room as well as the meeting attendees.

The resource, just like the other users scheduled for the meeting, would receive an appointment in its mailbox which could be accepted or declined by the owner.

When scheduling a resource, users can perform a busy search to see when the resource is available.

Even though a resource is assigned to a single post office, all users in your GroupWise system can schedule the resource.

Resources can receive all item types (mail messages, phone messages, appointments, tasks, and notes). Generally, if your purpose in defining resources is to allow them to be scheduled through GroupWise, they will only receive appointments.

Resource Owners

When you create a resource, you assign an owner to it. The owner must belong to the same post office as the resource and will be responsible for accepting or declining requests to schedule the resource. The owner can do this by proxying the resource's mailbox and physically opening the scheduling requests, or by setting up rules to manage the resource automatically.

The owner automatically receives proxy rights to the resource's mailbox. The owner can also grant proxy rights to another user to manage the resources.

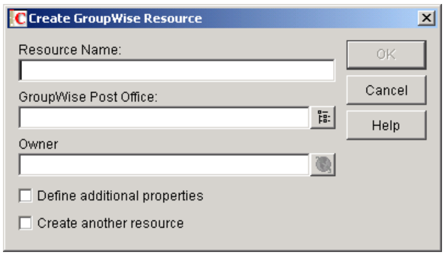
For information about how owners can manage resources, see "Owning Resources" in "Managing Your Mailbox" in the *GroupWise 6.5 Windows Client User Guide*.

Planning Resources

Before creating a new resource, make sure that the user who will own the resource has been created and belongs to the same post office where you are planning to create the resource.

Creating a New Resource

1 In ConsoleOne®, right-click the container where you want to create the Resource object > click New > Resource to display the Create GroupWise Resource dialog box.


Create GroupWise Resource
Resource Name:
OK
Cancel
GroupWise Post Office:
Help
Owner
□ Define additional properties
□ Create another resource

2 Fill in the following fields:

Resource Name: Enter a descriptive name. Because the name is used as part of the resource's GroupWise address, do not use any of the following invalid characters in the resource name:

ASCII characters 0-13

Asterisk *

At sign @

Braces { }

Colon :

Comma ,

Double quote "

Extended characters

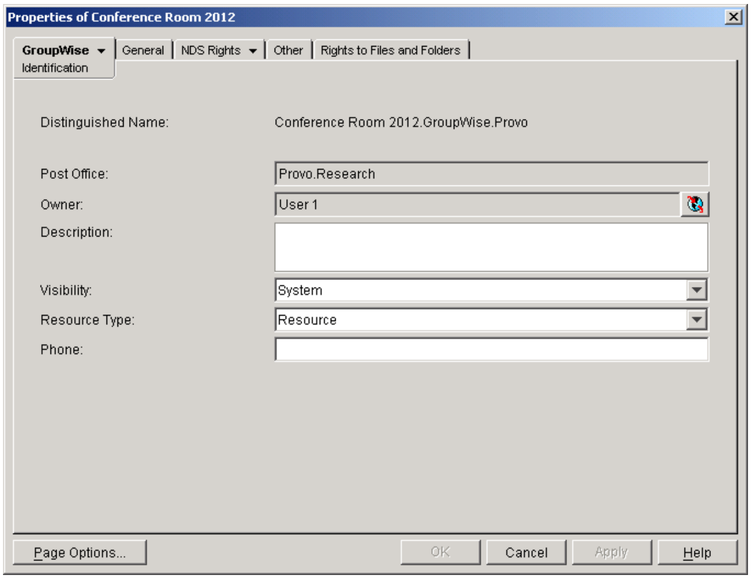
Parentheses ( )

Period .

GroupWise Post Office: Select the post office where the resource will be located.

Owner: Select the user who will be responsible for accepting or declining requests to use the resource. The owner must have a GroupWise account on the same post office as the resource.

3 Select Define Additional Properties, then click OK.



Properties of Conference Room 2012

Distinguished Name: Conference Room 2012.GroupWise.Provo

Post Office: Provo.Research

Owner: User 1

Description:

Visibility: System

Resource Type: Resource

Phone:

4 On the Identification page, fill in the following fields:

Description: Enter a description that will help users identify the use of the resource. The description will be displayed if the user chooses to view information about the resource in the Address Book.

If you define the resource type as a place, the description is automatically added to the Place field in the appointment. A good description can help users locate the place more easily.

Visibility: Select the level at which the resource will be visible in the Address Book. System causes the resource to be visible to all users in your GroupWise system. Domain causes the resource to be visible to all users in the same domain as the resource. Post Office causes the resource to be visible to all users on the same post office as the resource. None causes the resource to not be visible at any level. However, even if the resource is not displayed in a user's Address Book, he or she can schedule the resource by typing the resource name in an appointment's To field.

Type: You can identify the resource as a general resource or as a place. When a user schedules a resource that is defined as a place, the resource description is automatically added to the Place field in the appointment.

Phone: If the resource has a telephone number associated with it, such as a conference room with a telephone number, enter the phone number.

5 Click OK to save the resource information.

16 Managing Resources

The following sections provide information to help you manage the resources in your GroupWise® system:

- "Changing a Resource's Owner" on page 227
- "Adding a Resource to a Distribution List" on page 228
- "Moving a Resource" on page 229
- "Renaming a Resource" on page 230
- "Deleting a Resource" on page 230
- "Managing E-Mail Addresses" on page 230

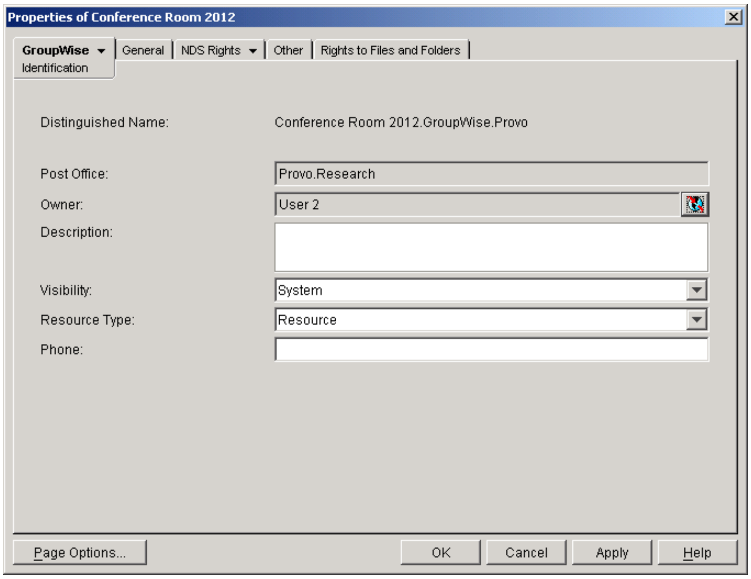
A resource's mailbox, just like a user's mailbox, is a combination of the information stored in its user database and the message databases located at its post office. Occasionally, you might want to perform maintenance tasks on the resource's mailbox to ensure the integrity of the databases. For details about performing maintenance on a resource's mailbox, see Chapter 27, "Maintaining User/Resource and Message Databases," on page 353.

Changing a Resource's Owner

You can change a resource's owner whenever necessary. The owner must be a user assigned to the same post office as the resource. If you need to give ownership of the resource to a user on a different post office, you must move the resource to that post office. For details, see "Moving a Resource" on page 229.

The new owner automatically receives proxy rights to the resource's mailbox. Proxy rights are removed for the old owner.

1 In ConsoleOne®, right-click the Resource object, then click Properties.



Properties of Conference Room 2012

Distinguished Name: Conference Room 2012.GroupWise.Provo

Post Office: Provo.Research

Owner: User 2

Description:

Visibility: System

Resource Type: Resource

Phone:

2 On the Identification page, browse to and select the new owner, then click OK to display the user's name in the Owner field.

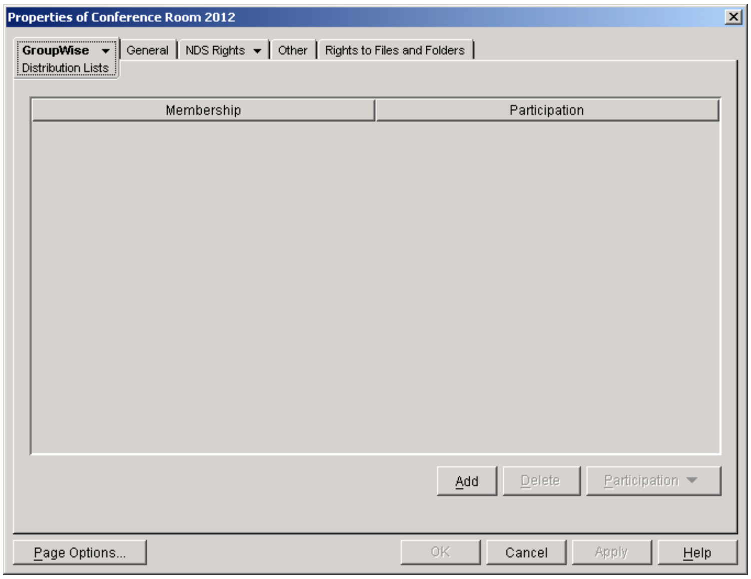
3 Click OK to save your changes.

Adding a Resource to a Distribution List

Just like users, resources can be added to distribution lists.

1 In ConsoleOne, right-click the Resource object, then click Properties.

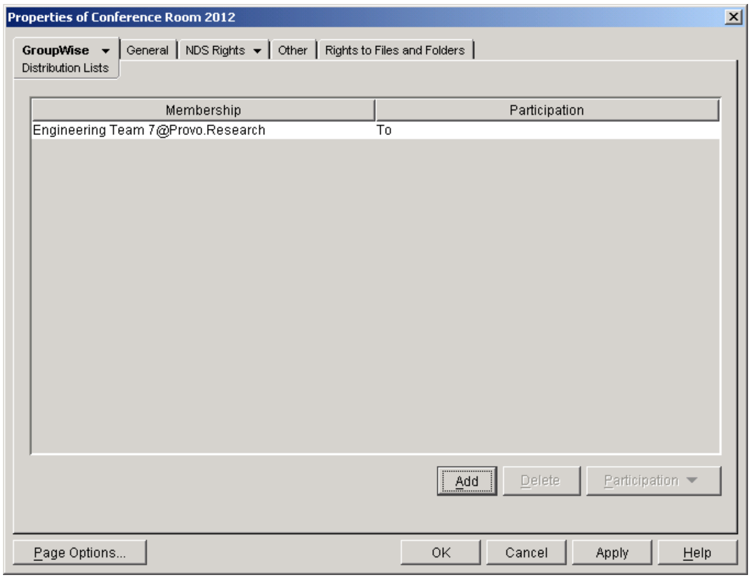
2 Click GroupWise > Distribution Lists to display the Distribution Lists page.



Properties of Conference Room 2012

Membership	Participation

3 Click Add, select the distribution list that you want to add the resource to, then click OK.



Membership	Participation
Engineering Team 7@Provo.Research	To

By default, the resource is added as a primary recipient (To: recipient).

4 If you want to change the resource's recipient type, select the distribution list, click Participation, then click To, CC, or BC.

5 Click OK to save your changes.

Moving a Resource

If necessary, you can move a resource from one post office to another. For example, you might need to move a resource if you are removing the resource's post office or if you need to reassign ownership of the resource to a user on another post office.

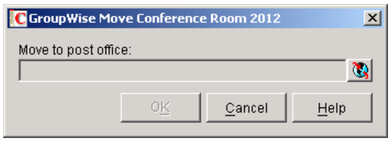
The resource retains the same name in the new post office as it has in the current post office. If another user, resource, or distribution list assigned to the new post office has the same name, you will need to rename one of them before you move the resource. For details, see "Renaming a Resource" on page 230.

When you move the resource, all items in its mailbox are moved to the new post office, which means that all schedules for the resource are kept intact.

To move a resource:

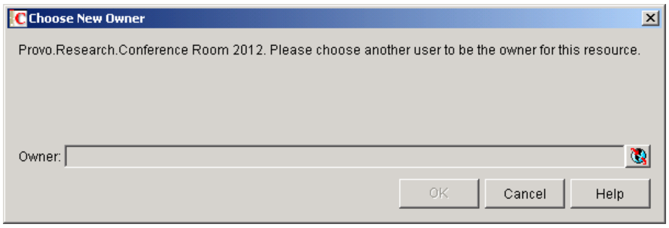
1 In ConsoleOne, right-click the Resource object in the GroupWise View, then click Move to display the GroupWise Move dialog box.

IMPORTANT: You must select the Resource object in the GroupWise View. If you select the object in the standard ConsoleOne View, you will move the Resource object from one container to another, not the resource from one post office to another.



Move to post office:

2 Select the post office to which you want to move the resource, then click OK to display the Choose New Owner dialog box.



Provo.Research.Conference Room 2012. Please choose another user to be the owner for this resource.

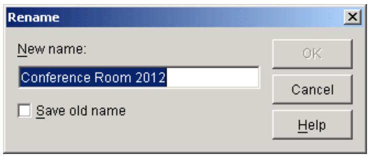
Owner:

3 Select the user who will be the resource's owner, then click OK to move the resource.

Renaming a Resource

Situations might arise where you need to give a resource a new name. For example, you might need to move the resource to another post office that already has a user, resource, or distribution list with the same name.

1 In ConsoleOne, right-click the Resource object in the GroupWise View, then click Rename to display the Rename dialog box



New name: Conference Room 2012

□ Save old name

2 In the New Name field, enter the new name for the resource.

3 Make sure the Save Old Name box is not checked. Saving the old name will cause duplicate resources to appear in the Address Book.

4 Click OK to rename the resource.

Deleting a Resource

When you delete a resource, all information is removed for the resource, including any schedules that have been established for the resource.

1 In ConsoleOne, right-click the Resource object, then click Delete.

2 Click Yes to confirm the deletion.

Managing E-Mail Addresses

To ensure that resource addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for resources. The following sections provide details:

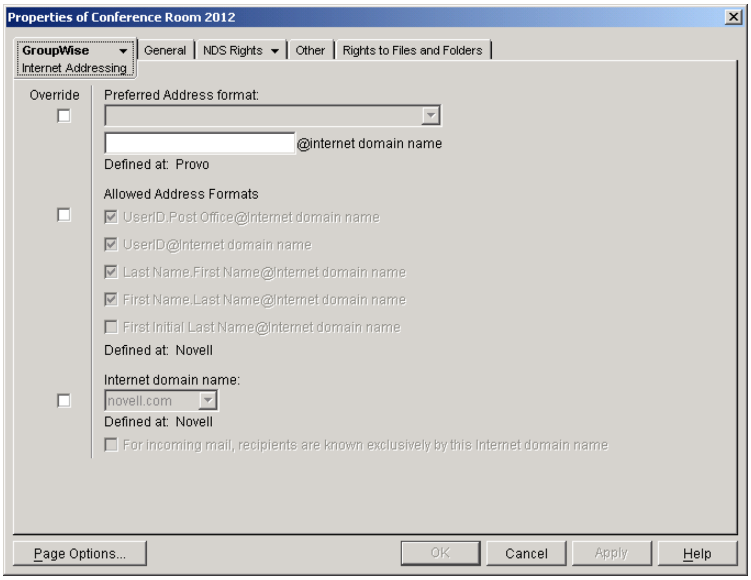
- "Changing a Resource's Internet Addressing Settings" on page 231
- "Changing a Resource's Visibility in the Address Book" on page 232
- "Creating a Nickname for a Resource" on page 233

Changing a Resource’s Internet Addressing Settings

By default, a resource inherits its Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from its post office, domain, or GroupWise system. If necessary, you can override these settings.

1 In ConsoleOne, right-click the Resource object, then click Properties.

2 Click GroupWise, then click Internet Addressing to display the Internet Addressing page.



Override

□ Preferred Address format:

@internet domain name

Defined at: Provo

□ Allowed Address Formats

☑ UserID.Post Office@Internet domain name

☑ UserID@Internet domain name

☑ Last Name.First Name@Internet domain name

☑ First Name.Last Name@Internet domain name

□ First Initial Last Name@Internet domain name

Defined at: Novell

□ Internet domain name: novell.com

Defined at: Novell

□ For incoming mail, recipients are known exclusively by this Internet domain name

3 To override one of the settings, select the Override box, then change the setting.

Preferred Address Format: The preferred address format determines how the resource’s address will be displayed in the GroupWise Address Book and in sent messages.

At the resource level, only three preferred address formats are available. The address formats that include first name, last name, and first initial do not apply to resource, so they are not available.

You can completely override the address format by explicitly defining the user portion of the address (*user@Internet domain name*). The user portion can include any RFC-compliant characters (no spaces, commas, and so forth).

Allowed Address Formats: The allowed address formats determine which address formats can be used to send messages to the resource.

Only the *UserID.Post Office@Internet domain name* and *UserID@Internet domain name* formats are valid for resources. The formats that include first name, last name, and first initial are not valid.

For example, using R1 as the resource ID, Research as the post office, and novell.com as the Internet domain, if you select the two valid formats, the resource would receive messages sent using either of the following addresses:

r1.research@novell.com
r1@novell.com

Internet Domain Name: The Internet domain name, along with the preferred address format, is used when constructing the e-mail address that is displayed in the GroupWise Address Book and in the To field of sent messages.

Only the Internet domain names that have been defined are displayed in the list. Internet domain names must be defined at the system level (Tools menu > GroupWise System Operations > Internet Addressing). For more information, see "Internet-Style Addressing" on page 87.

If you override the Internet domain name, the For Incoming Mail, Recipients are Known Exclusively by This Internet Domain Name becomes available. Enable this option if you only want the resource to be able to receive messages addressed with this Internet domain name. If you don't enable this option, the resource will receive messages addressed using any of the Internet domain names assigned to your GroupWise system.

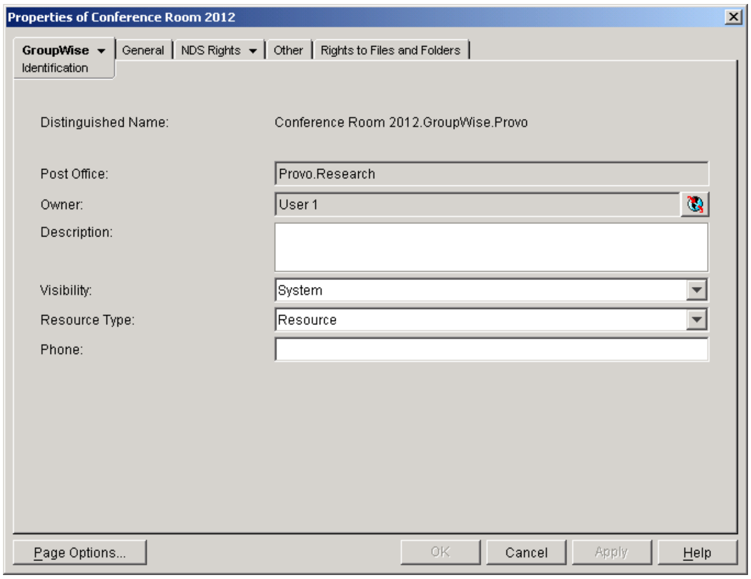
4 Click OK to save your changes.

Changing a Resource's Visibility in the Address Book

A resource's visibility level determines which users see the resource in their Address Books. You can control the availability of a resource by displaying it in the Address Books of all users in your GroupWise system, in the Address Books of those users in the resource's domain only, in the Address Books of those users on the resource's post office only, or in no Address Books. Even if the resource is not displayed in their Address Books, users can schedule the resource if they know the resource's name.

To change a resource's visibility:

1 In ConsoleOne, right-click the Resource object, then click Properties.



Distinguished Name: Conference Room 2012.GroupWise.Provo

Post Office: Provo.Research

Owner: User 1

Description:

Visibility: System

Resource Type: Resource

Phone:

2 In the Visibility field, select the desired visibility level.

System: The resource will be displayed in the Address Books of all users in your GroupWise system.

Domain: The resource will be displayed in the Address Books of all users in the resource's domain.

Post Office: The resource will be displayed in the Address Books of all users on the resource's post office.

None: The resource will not be displayed in any Address Books. Users will need to know the resource's name to schedule it.

3. Click OK to save your changes.

Creating a Nickname for a Resource

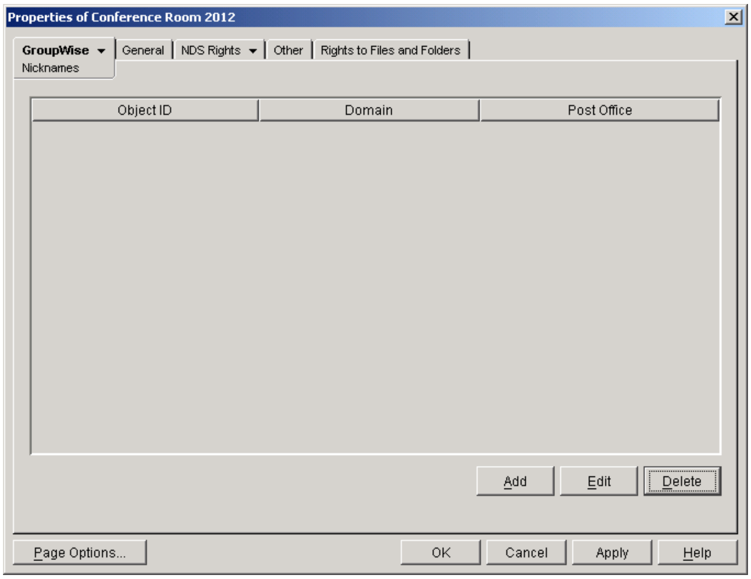
Each resource has a specific GroupWise address consisting of the resource's name, post office, and domain (*resource_name.post_office.domain*). You can assign one or more nicknames to a resource to give it an alternate address. Each part of the address (*resource_name*, *post_office*, and *domain*) can be different than the resource's actual address.

For example, you might want to create a nickname for a resource you have just moved (see "Moving a Resource" on page 229) or renamed (see "Renaming a Resource" on page 230). The nickname, which would be the resource's old address, would ensure that any appointments sent to the old address would be routed to the new address.

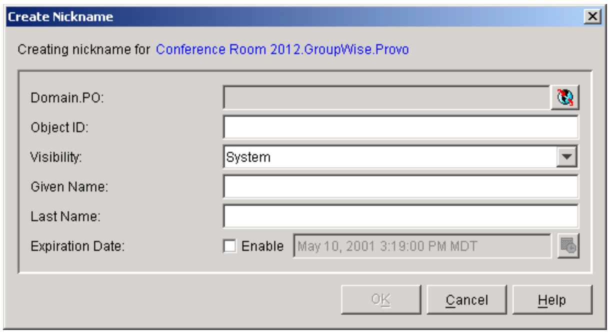
Nicknames are not displayed in the Address Book, which means users will need to know the nickname to use it. In addition, nicknames are not valid Internet addresses. For example, Internet users cannot schedule a resource by sending a message to *nickname@host*.

To create a nickname for a resource:

1. In ConsoleOne, right-click the Resource object, then click Properties.
2. Click GroupWise > Nicknames to display the Nicknames page.



3. Click Add to display the Create Nickname dialog box.


Create Nickname

Creating nickname for Conference Room 2012.GroupWise.Provo

Domain.PO:

Object ID:

Visibility: System

Given Name:

Last Name:

Expiration Date: □ Enable May 10, 2001 3:19:00 PM MDT

4 Fill in the following fields:

Domain.PO: Select the post office to which you want to assign the nickname. This can be any post office in your GroupWise system; it does not need to be the resource's post office.

Object ID: Enter the name to use as the *resource_name* portion of the nickname.

Visibility: Ignore this field. It is not used for nicknames.

Given Name: Ignore this field. It is not used for resource nicknames.

Last Name: Ignore this field. It is not used for resource nicknames.

Expiration Date: If you want the nickname to no longer work after a certain date, click Enable and then select the desired date.

5 Click OK to add the nickname to the list.

6 Click OK to save the changes to the Resource object.

VI Distribution Lists, Groups, and Organizational Roles

17 Understanding Distribution Lists, eDirectory Groups, and Organizational Roles

GroupWise distribution lists and Novell® eDirectory™ groups are sets of users and resources that can be addressed as a single entity. When a GroupWise user addresses an item (message, appointment, task, or note) to a distribution list, eDirectory group, or organization role, each user or resource that is a member receives a copy of the item.

The following sections provide information to help you learn about distribution lists, eDirectory groups, and organizational roles:

- "Public vs. Personal Address Lists" on page 237
- "Distribution Lists" on page 237
- "eDirectory Groups and Organizational Roles" on page 238

Public vs. Personal Address Lists

Distribution lists and eDirectory groups are public address lists, meaning that they are administrator-defined lists available to all users in your GroupWise system.

If users want to create personal address lists, they can create personal groups in the GroupWise client. When a user creates personal groups, the groups are saved in his or her mailbox and are available for use only by that user. They cannot be shared by, or transferred to, other users.

If a user wants to send to all users in a particular post office or domain, he or she can use wildcard addressing, if it has been enabled. See "Wildcard Addressing" on page 100.

Distribution Lists

A distribution list is specific to GroupWise. It is a public address list that you, as the GroupWise administrator, can create to facilitate easier addressing within your GroupWise system. Distribution lists can only contain users that have GroupWise accounts.

Each distribution list you want to create must be added as a Distribution List object in eDirectory. The name that you give the Distribution List object becomes the name by which the distribution list is displayed in the GroupWise Address Book.

Distribution list objects can be located in any eDirectory container that is in the same tree as the distribution list's domain.

Because a distribution list is an addressable entity, you must assign it to a post office when you create it. This ensures that the distribution list has a standard GroupWise address (*distribution_list_name.post_office.domain*).

Regardless of the distribution list's post office, all GroupWise users can use the distribution list when addressing a message.

You can determine which users see the distribution list in the Address Book. System visibility enables all users in your GroupWise system to see the distribution list. Domain visibility enables all users in the distribution list's domain to see the distribution list. Post Office visibility enables all users in the distribution list's post office to see the distribution list. Setting the visibility level to None means that no users will see the distribution list in the Address Book.

Users who cannot see the distribution list in the Address Book can still use the distribution list by typing the distribution list name in the To field of the message.

A distribution list can contain users and resources as well as other distribution lists, groups, and organizational roles. Members do not need to be on the same post office as the distribution list's post office.

For details about distribution lists, see Chapter 18, "Creating and Managing Distribution Lists," on page 239.

eDirectory Groups and Organizational Roles

eDirectory groups and organizational roles are general eDirectory objects that can be created to facilitate easier administration of eDirectory users who have common needs or who share a common role or responsibility.

If you have eDirectory groups or organizational roles that you want GroupWise users to be able to address messages to, you need to make them available in your GroupWise system. When doing so, you can choose the groups and roles that you want available, and choose which users they will be available to.

If a group or role contains both eDirectory users with GroupWise accounts and eDirectory users without GroupWise accounts, only those users with GroupWise accounts will receive messages addressed to the group or role.

As mentioned previously, Group and Organizational Role objects are not specific to GroupWise. For information about creating these objects, see your eDirectory documentation.

The name given to the Group object or Organizational Role object becomes the name by which the it is displayed in the GroupWise Address Book when you make it available. You make a group or role available in your GroupWise system by assigning it to a post office. This ensures that the group or role has a standard GroupWise address (*name.post_office.domain*). Regardless of the post office where the group or role is assigned, all GroupWise users can use it when addressing a message.

You can determine which users see the group or role in the Address Book. System visibility enables all users in your GroupWise system to see the group or role. Domain visibility enables all users in the distribution list's domain to see the group or role. Post Office visibility enables all users in the distribution list's post office to see the group or role. Setting the visibility level to None means that no users will see the group or role in the Address Book.

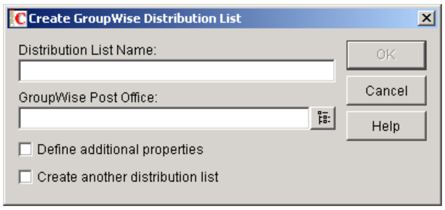
Users who cannot see the group or role in the Address Book can still use it by typing the name in the To field of the message.

18 Creating and Managing Distribution Lists

A GroupWise® distribution list can contain GroupWise users, resources, and other distribution lists. When creating the distribution list, you can determine each entry's participation in the list (primary recipient, carbon copy recipient, or blind copy recipient).

Creating a New Distribution List

1 In ConsoleOne®, right-click the eDirectory container where you want to create the Distribution List object, then click New > Distribution List.


Create GroupWise Distribution List
Distribution List Name:
GroupWise Post Office:
OK
Cancel
Help
□ Define additional properties
□ Create another distribution list

2 Fill in the following fields:

Distribution List Name: Enter a descriptive name. Because the name is used as part of the distribution list's GroupWise address, do not use any of the following invalid characters in the distribution list name:

ASCII characters 0-13

Asterisk *

At sign @

Braces { }

Colon :

Comma ,

Double quote "

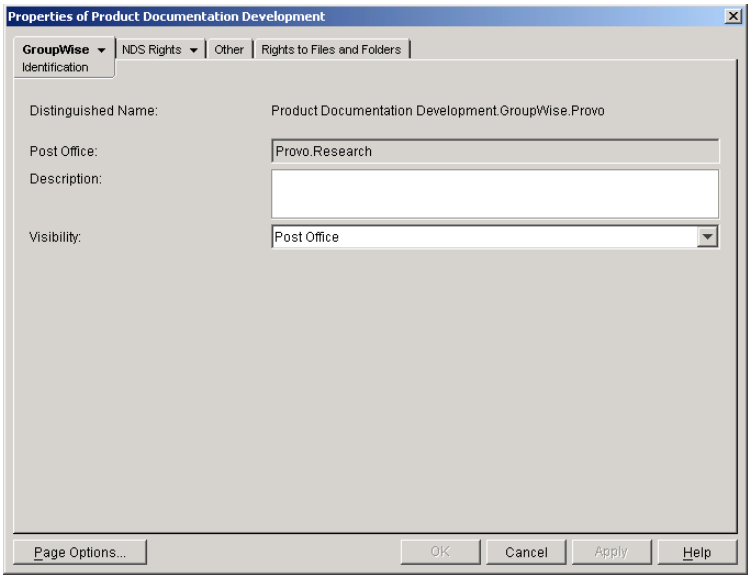
Extended characters

Parentheses ( )

Period .

GroupWise Post Office: Select the post office the distribution list will be assigned to. The distribution list can contain members of other post offices.

3 Select Define Additional Properties, then click OK.



Properties of Product Documentation Development

Distinguished Name: Product Documentation Development.GroupWise.Provo

Post Office: Provo.Research

Description:

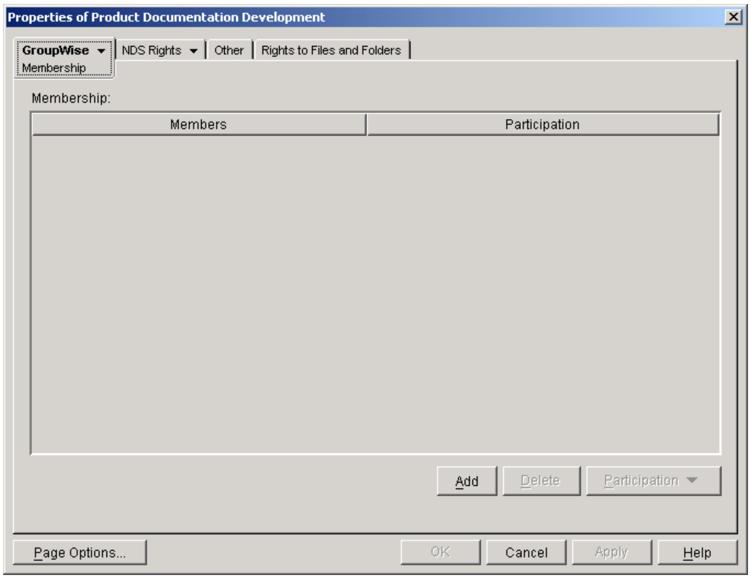
Visibility: Post Office

4 On the Identification page, fill in the following fields:

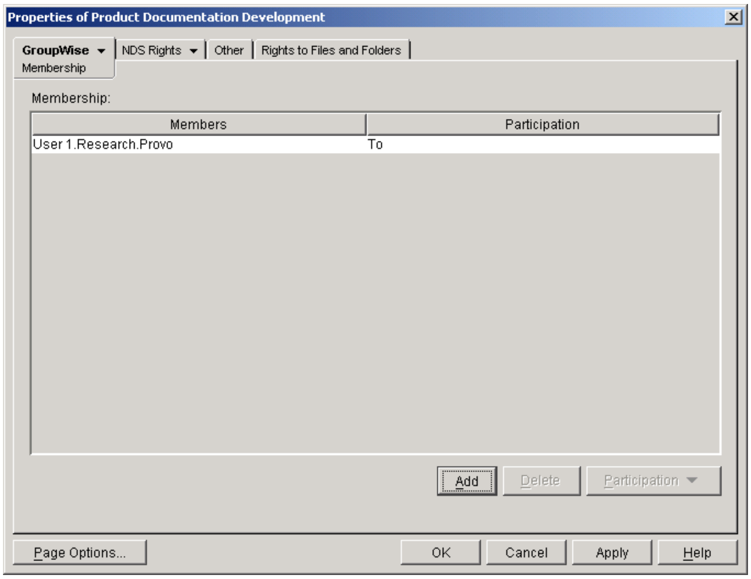
Description: Enter a description that will help you identify the purpose or members of the distribution list.

Visibility: Select the level at which the distribution list will be visible in the Address Book. System enables the distribution list to be visible to all users in your GroupWise system. Domain enables the distribution list to be visible to all users in the same domain as the distribution list. Post Office enables the distribution list to be visible to all users on the same post office as the distribution list. Setting the visibility level to None means that no users will see the distribution list in the Address Book. However, even if the distribution list is not displayed in a user's Address Book, he or she can use the distribution list by typing the distribution list's name in a message's To field.

5 Click GroupWise > Membership to display the Membership page.



6 Click Add, select the user, resource, distribution list, eDirectory group, or organizational role you want to add as a member, then click OK to add the member to the list.



Members	Participation
User 1.Research.Provo	To

By default, the member is added as a primary recipient (To: recipient).

7 If you want to change the member's recipient type, select the member, click Participation, then click To, CC, or BC.

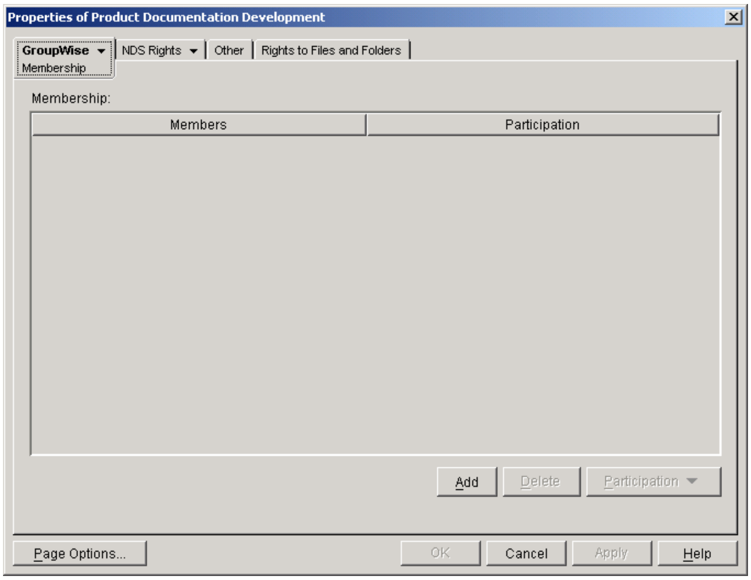
8 Repeat Step 6 and Step 7 to add additional members.

9 Click OK to save your changes.

Adding Members to a Distribution List

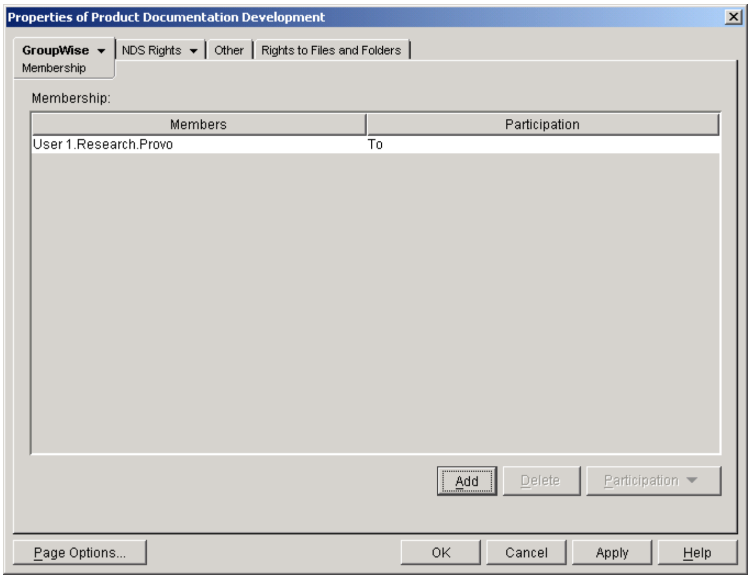
Distribution lists can contain users, resources, groups, organizational roles, and other distribution lists.

1. In ConsoleOne®, right-click the Distribution List object, then click Properties.
2. Click GroupWise > Membership to display the Membership page.



3. Click Add, select the user, resource, distribution list, group, or organizational role you want to add as a member, then click OK to add the member to the list.

   If you want to add an external user that is not listed for selection, see "Adding External Users to a Distribution List" on page 248.



Members	Participation
User 1.Research.Provo	To

   By default, the selected member is added as a primary recipient (To: recipient).

4. If you want to change the member's recipient type, select the member, click Participation, then click To, CC, or BC.
5. Repeat Step 3 and Step 4 to add additional members.
6. Click OK to save your changes.

Distribution lists much be managed by an administrator in ConsoleOne. However, GroupWise client users can create shared address books and then create groups within those shared address books so that the groups are available to all users with whom the address book is been shared. The creator of the shared address book can give other users read only rights, or can choose to grant them additional rights for adding, editing, and deleting information. For more information about shared address books, see "Sharing an Address Book with Another User" in "Using the Address Book" in the GroupWise 6.5 Windows Client User Guide.

Removing Members from a Distribution List

When you remove users' or resources' GroupWise accounts, delete groups, delete organizational roles, or delete distribution lists, they are automatically removed from any distribution lists in which they have membership.

To manually remove members from a distribution list:

1. In ConsoleOne, right-click the Distribution List object, then click Properties.
2. Click GroupWise > Membership to display the Membership page.
3. Select the member you want to remove from the list, then click Delete.

Moving a Distribution List

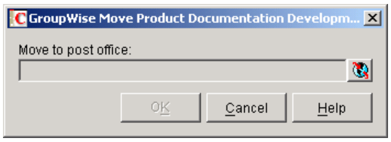
If necessary, you can move a distribution list from one post office to another. For example, you might need to move a distribution list from a post office you are removing.

The distribution list retains the same name on the new post office as it has on the current post office. If another user, resource, or distribution list assigned to the new post office has the same name, you will need to rename one of them before you move the distribution list. For details, see "Renaming a Distribution List" on page 244.

To move a distribution list:

1. In ConsoleOne, right-click the Distribution List object in the GroupWise View, then click Move to display the GroupWise Move dialog box.

   IMPORTANT: You must select the Distribution List object in the GroupWise View. If you select the object in the standard Console View, you will move the Distribution List object from one container to another, not the distribution list from one post office to another.



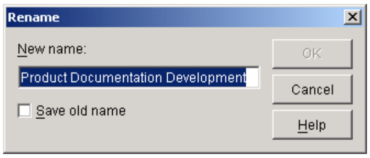
2. Select the post office to which you want to move the distribution list, then click OK to move the distribution list.

Renaming a Distribution List

Situations might arise where you need to give a distribution list a new name. For example, you might need to move the distribution list to another post office that already has a user, resource, or distribution list with the same name.

To rename a distribution list:

1. In ConsoleOne, right-click the Distribution List object in the GroupWise View, then click Rename to display the Rename dialog box.



New name: Product Documentation Development

☐ Save old name

2. In the New Name field, enter the new name for the distribution list.
3. Make sure the Save Old Name box is not checked. Saving the old name will cause duplicate distribution lists to appear in the Address Book.
4. Click OK to rename the distribution list.

Deleting a Distribution List

To delete a single distribution list:

1. In ConsoleOne, right-click the Distribution List object, then click Delete.
2. Click Yes to confirm the deletion.

To delete multiple distribution lists that belong to the same post office:

1. In ConsoleOne, right-click the Post Office object, then click Properties.
2. Click GroupWise > Distribution Lists.
3. Select one or more distribution lists, then click Delete.
4. Click OK to complete the deletion.

Managing E-Mail Addresses

To ensure that distribution list addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for distribution lists. The following sections provide details:

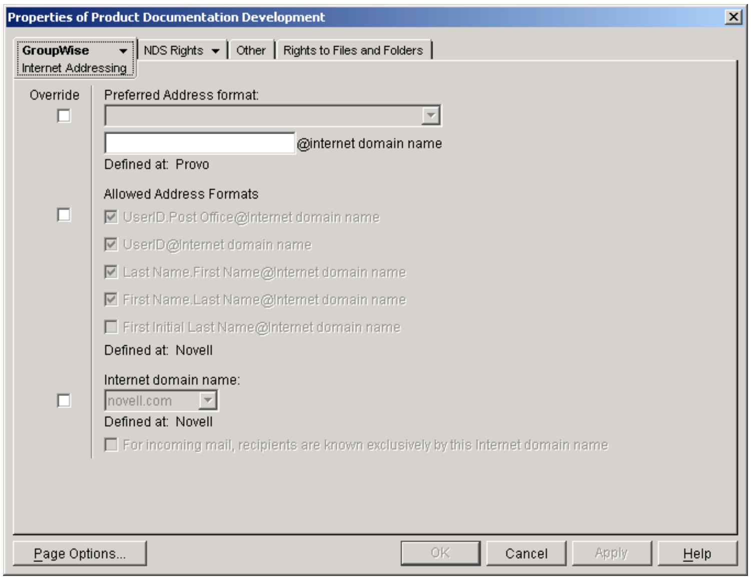
- "Changing a Distribution List's Internet Addressing Settings" on page 245
- "Changing a Distribution List's Visibility in the Address Book" on page 246
- "Creating a Nickname for a Distribution List" on page 247

Changing a Distribution List’s Internet Addressing Settings

By default, a distribution list inherits its Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from its post office, domain, or GroupWise system. If necessary, you can override these settings for a distribution list.

1 In ConsoleOne, right-click the Distribution List object, then click Properties.

2 Click GroupWise, then click Internet Addressing to display the Internet Addressing page.



Override

□ Preferred Address format:

@internet domain name

Defined at: Provo

□ Allowed Address Formats

☑ UserID.Post Office@Internet domain name

☑ UserID@Internet domain name

☑ Last Name.First Name@Internet domain name

☑ First Name.Last Name@Internet domain name

□ First Initial Last Name@Internet domain name

Defined at: Novell

□ Internet domain name: novell.com

Defined at: Novell

□ For incoming mail, recipients are known exclusively by this Internet domain name

3 To override one of the settings, select the Override box, then change the setting.

Preferred Address Format: The preferred address format determines how the distribution list’s address will be displayed in the GroupWise Address Book and in sent messages.

At the distribution list level, only three preferred address formats are available. The address formats that include first name, last name, and first initial do not apply to distribution lists, so they are not available.

You can completely override the address format by explicitly defining the user portion of the address (*user@Internet domain name*). The user portion can include any RFC-compliant characters (no spaces, commas, and so forth).

Allowed Address Formats: The allowed address formats determine which address formats can be used to send messages to the distribution list.

Only the *UserID.Post Office@Internet domain name* and *UserID@Internet domain name* formats are valid for distribution lists. The formats that include first name, last name, and first initial are not valid.

For example, using DL1 as the distribution list ID, Research as the post office, and novell.com as the Internet domain, if you select the two valid formats, members of the distribution list would receive messages sent using either of the following addresses:

dl1.research@novell.com
dl1@novell.com

Internet Domain Name: The Internet domain name, along with the preferred address format, is used when constructing the e-mail address that is displayed in the GroupWise Address Book and in the To field of sent messages.

Only the Internet domain names that have been defined are displayed in the list. Internet domain names must be defined at the system level (Tools menu > GroupWise System Operations > Internet Addressing). For more information, see "Internet-Style Addressing" on page 87.

If you override the Internet domain name, the For Incoming Mail, Recipients are Known Exclusively by This Internet Domain Name becomes available. Enable this option if you only want the distribution list to be able to receive messages addressed with this Internet domain name. If you don't enable this option, the distribution list will receive messages addressed using any of the Internet domain names assigned to your GroupWise system.

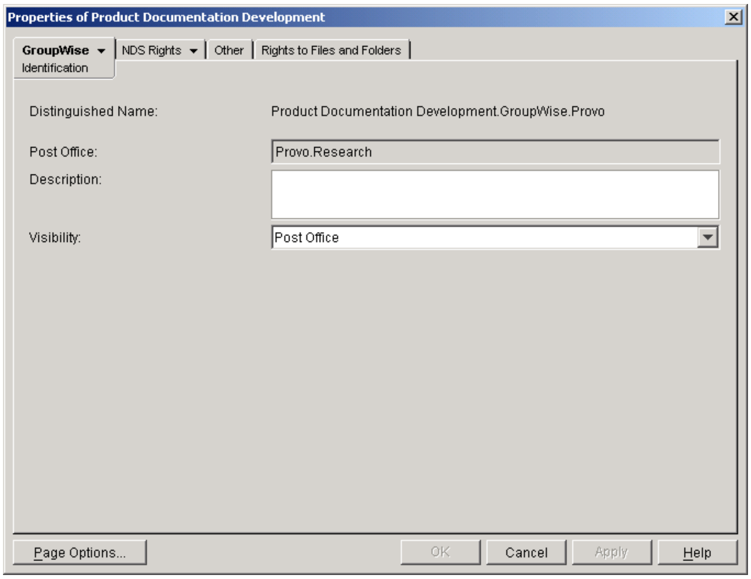
4 Click OK to save your changes.

Changing a Distribution List's Visibility in the Address Book

A distribution list's visibility level determines which users see the distribution list in the Address Books. You can control the availability of a distribution list by displaying it in the Address Book for all users in your GroupWise system, in the Address Book for those users in the distribution list's domain only, in the Address Book for those users on the distribution list's post office only, or not displaying it at all. Even if the distribution list is not displayed in the Address Book, users can use the distribution list if they know its name.

To change a distribution list's visibility:

1 In ConsoleOne, right-click the Distribution List object, then click Properties.


Properties of Product Documentation Development
GroupWise
Identification
NDS Rights
Other
Rights to Files and Folders
Page Options...
OK
Cancel
Apply
Help

Distinguished Name: Product Documentation Development.GroupWise.Provo

Post Office: Provo.Research

Description:

Visibility: Post Office

2 In the Visibility field, select the desired visibility level.

System: The distribution list will be displayed in the Address Book for all users in your GroupWise system.

Domain: The distribution list will be displayed in the Address Book for all users in the distribution list's domain.

Post Office: The distribution list will be displayed in the Address Book for all users on the distribution list's post office.

None: The distribution list will not be displayed in the Address Book. Users will need to know the distribution list's name to use it.

3 Click OK to save your changes.

Creating a Nickname for a Distribution List

Each distribution list has a specific GroupWise address consisting of the distribution list's name, post office, and domain (*distribution_list_name.post_office.domain*). You can assign one or more nicknames to a distribution list to give it an alternate address. Each part of the address (*distribution_list_name*, *post_office*, and *domain*) can be different than the distribution list's actual address.

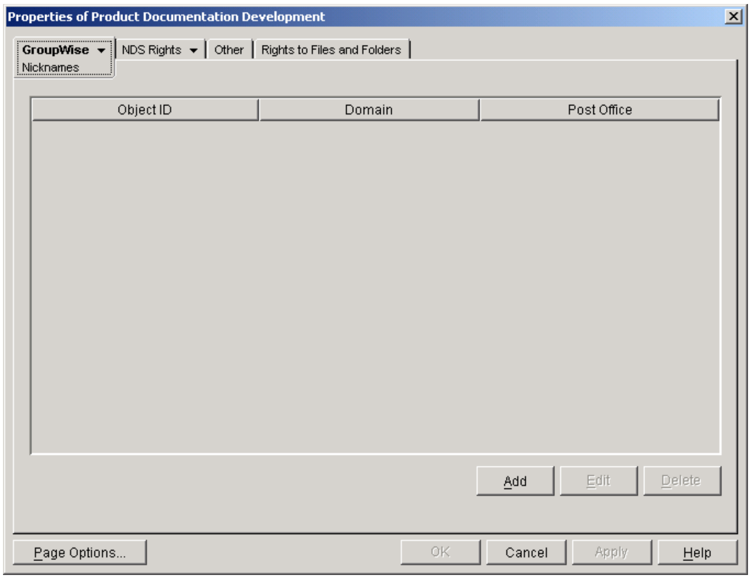
For example, you might want to create a nickname for a distribution list you have just moved (see "Creating a Nickname for a Distribution List" on page 247) or renamed (see "Renaming a Distribution List" on page 244). The nickname, which would be the distribution list's old address, would ensure that any use of the old address would result in the new address being used instead.

Nicknames are not displayed in the Address Book, which means users will need to know the nickname to use it. In addition, nicknames are not valid Internet addresses. For example, Internet users cannot address a message to *nickname@host*.

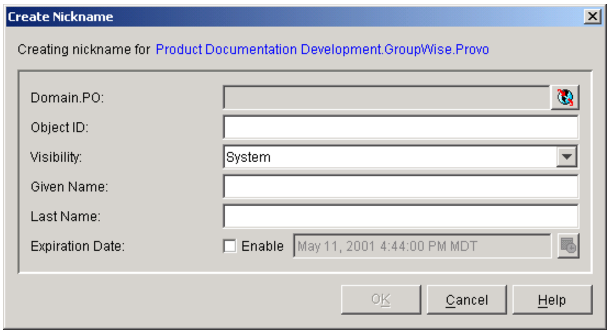
To create a nickname for a distribution list:

1 In ConsoleOne, right-click the Distribution List object, then click Properties.

2 Click GroupWise > Nicknames to display the Nicknames page.



3 Click Add to display the Create Nickname dialog box.



Create Nickname

Creating nickname for Product Documentation Development.GroupWise.Provo

Domain.PO:

Object ID:

Visibility: System

Given Name:

Last Name:

Expiration Date: □ Enable May 11, 2001 4:44:00 PM MDT

4 Fill in the following fields:

Domain.PO: Select the post office where you want to assign the nickname. This can be any post office in your GroupWise system; it does not have to be the distribution list's post office.

Object ID: Enter the name to use as the *distribution_list_name* portion of the nickname.

Visibility: Ignore this field. Nicknames are not displayed in the Address Book.

Given Name: Ignore this field. It is not used for distribution list nicknames.

Last Name: Ignore this field. It is not used for distribution list nicknames.

Expiration Date: If you want the nickname to no longer work after a certain date, click Enable and then select the desired date.

5 Click OK to add the nickname to the list.

6 Click OK to save the changes to the Distribution List object.

Adding External Users to a Distribution List

Members of distribution lists must have corresponding eDirectory objects. If you want to add user to a distribution list that do not belong to your GroupWise system, you must create objects to represent these external users within your GroupWise system.

- "Creating an External Domain" on page 248
- "Creating an External Post Office" on page 248
- "Creating an External User" on page 249

Creating an External Domain

You create an external domain to represent the world outside your GroupWise system.

1 In ConsoleOne, right-click GroupWise System, then click New > External Domain.

2 Provide a unique name for the domain, then click OK.

Creating an External Post Office

You create an external post office in the external domain to hold External User objects.

1 In ConsoleOne, right-click the External Domain object, then click New > External Post Office.

2 Provide a unique name for the post office, then click OK.

Creating an External User

You create an external user so that it can be selected when adding members to a distribution list.

1. In ConsoleOne, right-click the External Post Office object, then click New > External User.
2. Provide a unique name for the user, then click OK.
3. Right-click the new External User object, then click Properties.
4. On the Identification page, fill in at least the first and last names.
5. Click GroupWise > Internet Addressing.
6. Select Override.
7. Select the preferred addressing format depending on how you want e-mail to this user to be addressed.

   or

   Provide a custom address format.
8. Click OK to save the user information.
9. Follow the instructions in "Adding Members to a Distribution List" on page 242 to add the external user to a distribution list.

19 Using eDirectory Groups as Distribution Lists

Novell® eDirectory™ groups can be configured to function as GroupWise® distribution lists.

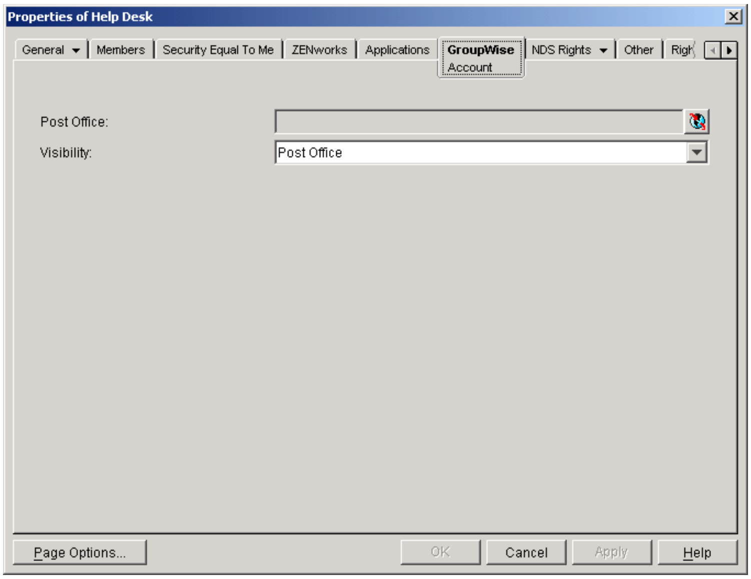
- "Setting Up an eDirectory Group for Use in GroupWise" on page 251
- "Seeing Which Members of an eDirectory Group Have GroupWise Accounts" on page 252
- "Changing a Group's Visibility in the Address Book" on page 253
- "Moving a Group" on page 253
- "Renaming a Group" on page 254
- "Removing a Group from GroupWise" on page 254

Setting Up an eDirectory Group for Use in GroupWise

By default, eDirectory groups are not automatically available for use as distribution lists in GroupWise. To make an eDirectory group available, you need to assign it to a GroupWise post office.

1 In ConsoleOne®, right-click the Group object, then click Properties.

2 Click GroupWise > Account to display the Account page.



Post Office:

Visibility: Post Office

3 Fill in the following fields:

Post Office: Select the post office where you want to assign the group. You can choose any post office you want. If you plan to limit visibility of the group to users on a specific post office or in a specific domain, you should select that post office or a post office in the desired domain.

Visibility: Select the level at which the group will be visible in the Address Book. System enables the group to be visible to all users in your GroupWise system. Domain enables the group to be visible to all users in the same domain as the group. Post Office enables the group to be visible to all users on the same post office as the group. Setting the visibility to None means that the group will not be visible at any level. However, even if the group is not displayed in a user's Address Book, he or she can use the group by typing the group's name in a message's To field.

4 Click OK to save the changes.

The group is now treated like a GroupWise distribution list and is visible in the GroupWise View when you filter on distribution lists.

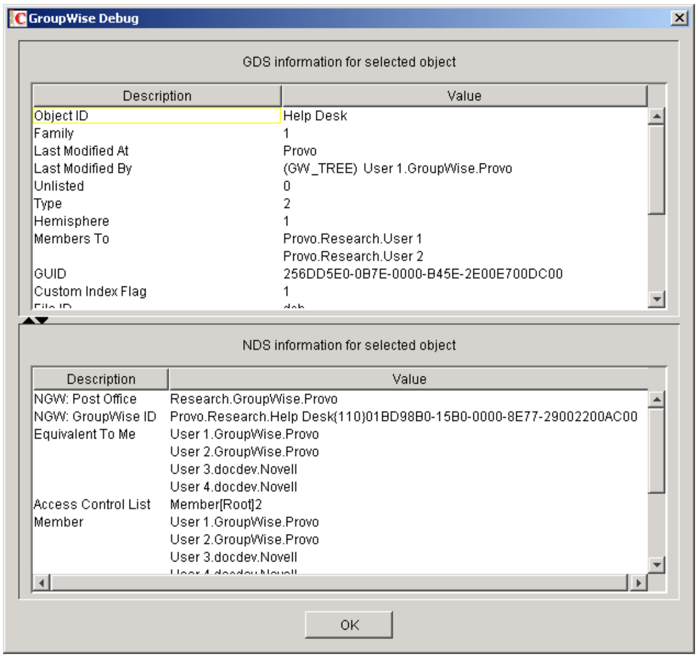
When GroupWise users send messages to the group, only those group members who have GroupWise accounts will receive messages.

Seeing Which Members of an eDirectory Group Have GroupWise Accounts

eDirectory groups can include members who have GroupWise accounts and members who do not have GroupWise accounts. When the group is used to address a message, only those members who have GroupWise accounts will receive the message.

To see which members have GroupWise accounts and which ones do not:

1 In ConsoleOne, select the Group object, then click Tools > GroupWise Diagnostics > Display Object.



GDS information for selected object

Description	Value
Object ID	Help Desk
Family	1
Last Modified At	Provo
Last Modified By	(GW_TREE) User 1.GroupWise.Provo
Unlisted	0
Type	2
Hemisphere	1
Members To	Provo.Research.User 1 Provo.Research.User 2
GUID	256DD5E0-0B7E-0000-B45E-2E00E700DC00
Custom Index Flag	1

NDS information for selected object

Description	Value
NGW: Post Office	Research.GroupWise.Provo
NGW: GroupWise ID	Provo.Research.Help Desk{110}01BD98B0-15B0-0000-8E77-29002200AC00
Equivalent To Me	User 1.GroupWise.Provo User 2.GroupWise.Provo User 3.docdev.Novell User 4.docdev.Novell
Access Control List	Member[Root]2
Member	User 1.GroupWise.Provo User 2.GroupWise.Provo User 3.docdev.Novell

The top window displays the members who have GroupWise accounts. The bottom window displays all members.

2 When you've finished viewing the information, click OK.

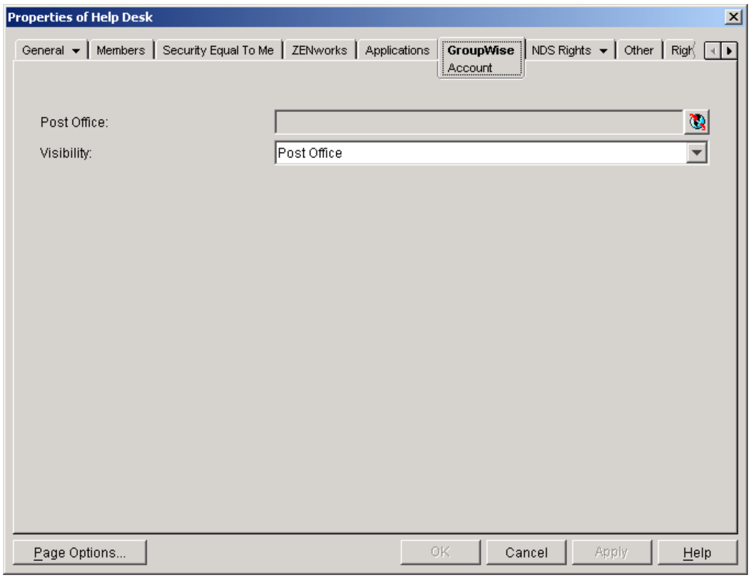
Changing a Group's Visibility in the Address Book

An eDirectory group's visibility level determines which users see the group in the Address Books. You can control the availability of a group by displaying it in the Address Book for all users in your GroupWise system, in the Address Book for those users in the group's domain only, in the Address Book for those users on the group's post office only, or not displaying it at all. Even if the group is not displayed in the Address Book, users can use the group if they know its name.

To change an eDirectory group's visibility in the GroupWise Address Book:

1 In ConsoleOne, right-click the Group object, then click Properties.

2 Click GroupWise > Account to display the Account page:



Post Office:

Visibility: Post Office

3 In the Visibility field, select the desired visibility level.

System: The group will be displayed in the Address Book for all users in your GroupWise system.

Domain: The group will be displayed in the Address Book for all users in the group's domain.

Post Office: The group will be displayed in the Address Book for all users on the group's post office.

None: The group will not be displayed in the Address Book. Users will need to know the group's name to use it.

4 Click OK to save your changes.

Moving a Group

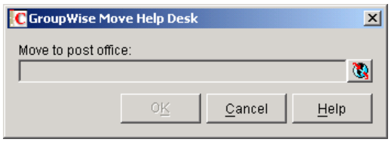
If necessary, you can move an eDirectory group from one post office to another. For example, you might need to move a group from a post office you are removing.

The group retains the same name on the new post office as it has on the current post office. If another object (user, resource, distribution list, group, or organizational role) assigned to the new post office has the same name, you will need to rename one of them before you move the group. For details, see "Renaming a Distribution List" on page 244.

To move an eDirectory group from one post office to another:

1 In ConsoleOne, right-click the Group object in the GroupWise View, then click Move to display the GroupWise Move dialog box.

IMPORTANT: You must select the Group object in the GroupWise View. If you select the object in the standard Console View, you will move the Group object from one eDirectory container to another, not the group from one post office to another.



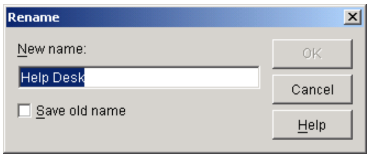
2 Select the post office to which you want to move the group, then click OK to move the group.

Renaming a Group

Situations might arise where you need to give an eDirectory group a new name. For example, you might need to move the group to another post office that already has an object (user, resource, distribution list, group, or organizational unit) with the same name.

When you rename an eDirectory group, you rename the Group object. This means that not only are you changing the name in GroupWise, but also in eDirectory.

1 In ConsoleOne, right-click the Group object, then click Rename to display the Rename dialog box.



2 In the New Name field, enter the new name for the group.

3 Make sure the Save Old Name box is not checked. Saving the old name will cause duplicate groups to appear in the Address Book.

4 Click OK to rename the group.

Removing a Group from GroupWise

If you decide that you no longer want an eDirectory group to be a distribution list in GroupWise, you can remove its association with a GroupWise post office, so that it returns to being just an eDirectory group.

1 In ConsoleOne, right-click the Group object, click Delete, then click Yes to confirm that you want to delete the object.

2 In the eDirectory Account box, deselect Delete to retain the Group object in eDirectory.

The Delete option in the GroupWise Account box is selected by default and cannot be deselected.

3 Click OK twice to complete the deletion.

20 Using Organizational Roles as GroupWise Distribution Lists

Organizational roles can be configured to function as GroupWise distribution lists.

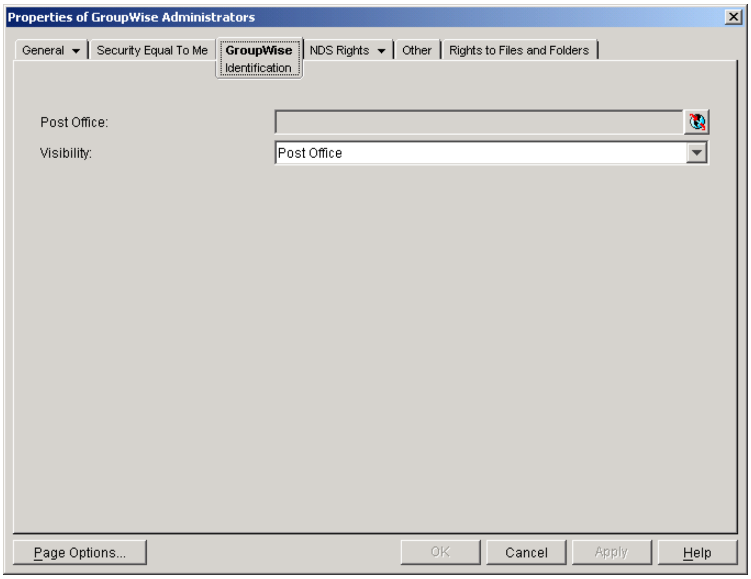
- "Setting Up an Organizational Role as a GroupWise Distribution List" on page 255
- "Seeing Which Members of an Organizational Role Have GroupWise Accounts" on page 256
- "Changing an Organizational Role's Visibility in the Address Book" on page 257
- "Moving an Organizational Role" on page 258
- "Renaming an Organizational Role" on page 258
- "Removing an Organizational Group from GroupWise" on page 259

Setting Up an Organizational Role as a GroupWise Distribution List

By default, Novell® eDirectory™ organizational roles are not automatically available for use as distribution lists in GroupWise®. To make an organizational role available, you need to assign it to a GroupWise post office.

1 In ConsoleOne®, right-click the Organizational Role object, then click Properties.

2 Click the GroupWise tab to display the Identification page.



Properties of GroupWise Administrators

Post Office:

Visibility: Post Office

3 Fill in the following fields:

Post Office: Select the post office where you want to assign the organizational role. You can choose any post office you want. If you plan to limit visibility of the organizational role to users on a specific post office or in a specific domain, you should select that post office or a post office in the desired domain.

Visibility: Select the level at which the role will be visible in the Address Book. System enables the role to be visible to all users in your GroupWise system. Domain enables the role to be visible to all users in the same domain as the role. Post Office enables the role to be visible to all users on the same post office as the role. Setting the visibility to None means that the role will not be visible at any level. However, even if the role is not displayed in a user's Address Book, he or she can use the role by typing the role's name in a message's To field.

4. Click OK to save the changes.

The organizational role is now treated like a GroupWise distribution list and is visible in the GroupWise View when you filter on distribution lists.

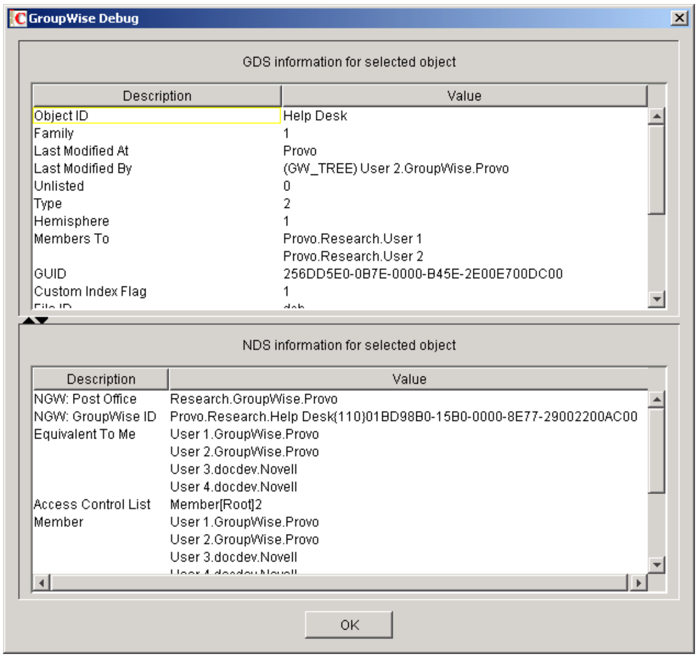
When GroupWise users send messages to the organization role, only those role members who have GroupWise accounts will receive messages.

Seeing Which Members of an Organizational Role Have GroupWise Accounts

eDirectory organizational roles can include members who have GroupWise accounts and members who do not have GroupWise accounts. When the organizational role is used to address a message, only those members who have GroupWise accounts will receive the message.

To see which members have GroupWise accounts and which ones do not:

1. In ConsoleOne, select the Organizational Role object, then click Tools > GroupWise Diagnostics > Display Object.



GroupWise Debug

GDS information for selected object

Description	Value
Object ID	Help Desk
Family	1
Last Modified At	Provo
Last Modified By	(GW_TREE) User 2.GroupWise.Provo
Unlisted	0
Type	2
Hemisphere	1
Members To	Provo.Research.User 1 Provo.Research.User 2
GUID	256DD5E0-0B7E-0000-B45E-2E00E700DC00
Custom Index Flag	1
File ID	deb

NDS information for selected object

Description	Value
NGW: Post Office	Research.GroupWise.Provo
NGW: GroupWise ID	Provo.Research.Help Desk{110}01BD98B0-15B0-0000-8E77-29002200AC00
Equivalent To Me	User 1.GroupWise.Provo User 2.GroupWise.Provo User 3.docdev.Novell User 4.docdev.Novell
Access Control List	Member[Root]2
Member	User 1.GroupWise.Provo User 2.GroupWise.Provo User 3.docdev.Novell User 4.docdev.Novell

The top window displays the members who have GroupWise accounts. The bottom window displays all members.

2 When you've finished viewing the information, click OK.

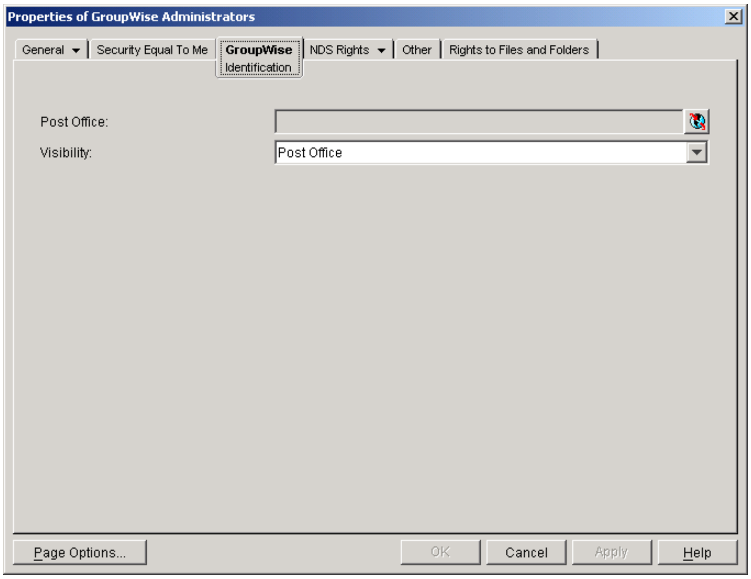
Changing an Organizational Role's Visibility in the Address Book

An organizational role's visibility level determines which users see the role in the Address Books. You can control the availability of a role by displaying it in the Address Book for all users in your GroupWise system, in the Address Book for those users in the role's domain only, in the Address Book for those users on the role's post office only, or not displaying it at all. Even if the organizational role is not displayed in the Address Book, users can use the role if they know its name.

To change an organizational role's visibility in the GroupWise Address Book:

1 In ConsoleOne, right-click the Organizational Role object, then click Properties.

2 Click GroupWise > Identification to display the Identification page:



Properties of GroupWise Administrators

Post Office:

Visibility: Post Office

3 In the Visibility field, select the desired visibility level.

System: The organizational role will be displayed in the Address Book for all users in your GroupWise system.

Domain: The organizational role will be displayed in the Address Book for all users in the role's domain.

Post Office: The organizational role will be displayed in the Address Book for all users on the role's post office.

None: The organizational role will not be displayed in the Address Book. Users will need to know the role's name to use it.

4 Click OK to save your changes.

Moving an Organizational Role

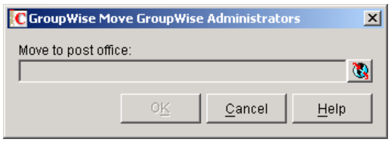
If necessary, you can move an organizational role from one post office to another. For example, you might need to move an organizational role from a post office you are removing.

The organizational role retains the same name on the new post office as it has on the current post office. If another object (user, resource, distribution list, group, or organizational role) assigned to the new post office has the same name, you will need to rename one of them before you move the organizational role. For details, see "Renaming a Distribution List" on page 244.

To move an organizational role from one post office to another:

1 In ConsoleOne, right-click the Organizational Role object in the GroupWise View, then click Move to display the GroupWise Move dialog box.

IMPORTANT: You must select the Organizational Role object in the GroupWise View. If you select the object in the standard Console View, you will move the Organizational Role object from one eDirectory container to another, not the group from one post office to another.



2 Select the post office to which you want to move the organizational role, then click OK to move the organizational role.

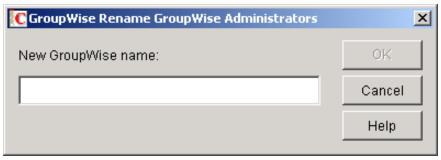
Renaming an Organizational Role

Situations might arise where you need to give an organizational role a new name. For example, you might need to move the organizational role to another post office that already has an object (user, resource, distribution list, group, or organizational unit) with the same name.

When you rename an organizational role, you rename the Organizational Role object. This means that you are not only changing the name in GroupWise, but also in eDirectory.

To rename an organizational role:

1 In ConsoleOne, right-click the Organizational Role object, then click Rename to display the GroupWise Rename dialog box.



2 In the New Name field, enter the new name for the organizational role.

3 Click OK to rename the organizational role.

Removing an Organizational Group from GroupWise

If you decide that you no longer want an organizational role to be a public address list in GroupWise, you can remove its association with a GroupWise post office, so that it returns to being just an eDirectory organizational role.

1. In ConsoleOne, right-click the Organizational Role object, click Delete, then click Yes to confirm that you want to delete the object.
2. In the eDirectory Account box, deselect Delete to retain the Organizational Role object in eDirectory.

   The Delete option in the GroupWise Account box is selected by default and cannot be deselected.
3. Click OK twice to complete the deletion.

VII Libraries and Documents

21 Document Management Services Overview

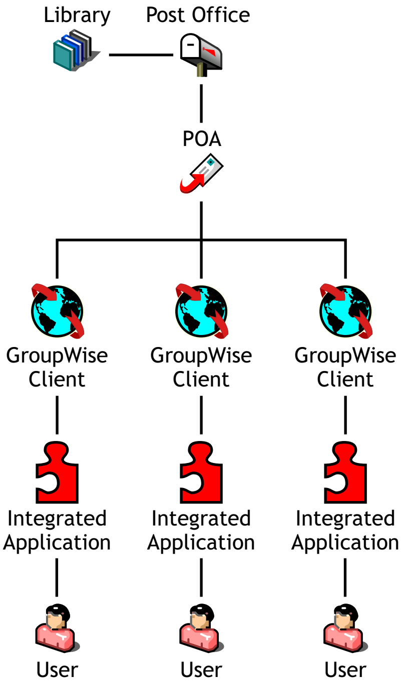
GroupWise® Document Management Services (DMS) lets users create documents with integrated applications, save them, then easily locate a specific document later without knowing the application, a specific document name, or the document's physical location. Users can create, share, locate, edit, view, and check out documents that are created under the management of GroupWise DMS.

A GroupWise DMS system consists of the following components:

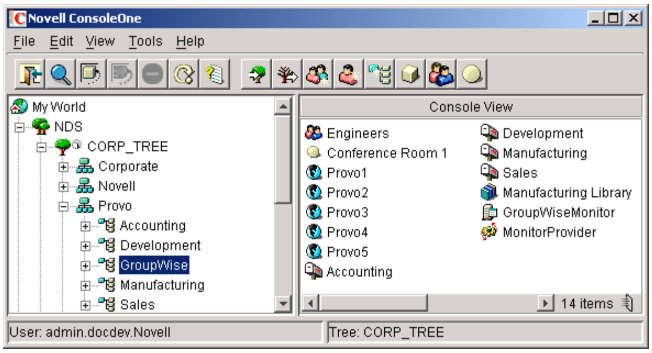
- "Libraries" on page 263
- "Document Storage Areas" on page 265
- "Documents" on page 265
- "Integrations" on page 268

Libraries

A library is a set of documents and a database that allows the set of documents to be managed as a unit. A library must belong to a specific post office but can be accessed by users in other post offices. The GroupWise client enables users to store and manage their documents in the library. The GroupWise Post Office Agent (POA) transfers documents between the GroupWise client and the library.



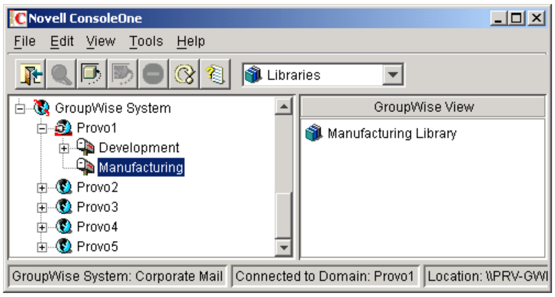
In ConsoleOne®, a library can be viewed where it resides in the Novell® eDirectory™ tree.



User: admin.docdev.Novell

Tree: CORP_TREE

A library can also be viewed in relationship to the post office that owns it.

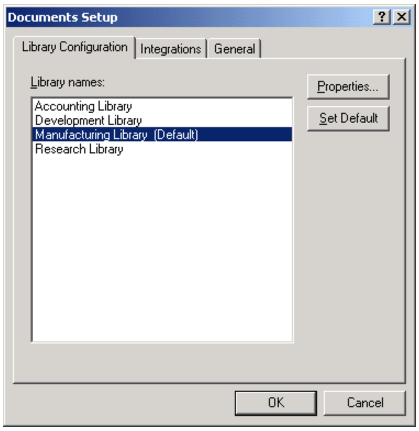


GroupWise System: Corporate Mail

Connected to Domain: Provo1

Location: \\PRV-GWI

In the GroupWise Windows client, users can view a list of all the libraries to which they have access by clicking Tools > Options > Documents.



Library names:

Accounting Library
Development Library
Manufacturing Library (Default)
Research Library

NOTE: This feature is not available in the Cross-Platform client.

Physically, a library consists of a set of directories and databases stored in the gwdms subdirectory of the post office, as illustrated in "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

For complete information on libraries, see Chapter 22, "Creating and Managing Libraries," on page 269

Document Storage Areas

Documents can be stored at the post office, as illustrated in "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. This is the simplest configuration, but it is not recommended for libraries where substantial growth is anticipated because documents stored at the post office cannot easily be moved to a different location where additional storage space is available.

Preferably, documents should be stored outside the post office, in document storage areas. Document storage areas are physical locations, such as drive volumes, optical devices, hard drives on other servers, and so on. Document storage areas can be located anywhere that the POA can access them locally or using direct network access (mapped drive or mounted file system).

A document storage area has the same internal directory structure that is used to store documents at the post office. The only difference is that a document storage area can be located anywhere in your system. Therefore, a document storage area can be moved easily, so it is easy to expand your document storage capacity if you store documents in a document storage area rather than at the post office.

For complete information on document storage areas, see "Managing Document Storage Areas" on page 290.

Documents

Documents created using GroupWise DMS are not stored as individual files. Instead, documents are stored in database structures called binary large objects (BLOBs). A document and all of its versions are stored in the separate BLOB files. BLOBs are compressed (50% or more) to conserve storage space. BLOBs are encrypted to provide security.

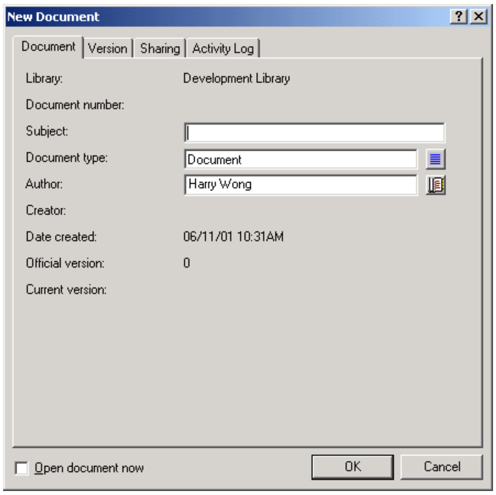
Because documents are stored in a database structure, information can be associated with each document that is not part of the document itself, such as:

- "Document Properties" on page 265
- "Document Types" on page 266

For complete information on documents, see Chapter 23, "Creating and Managing Documents," on page 303.

Document Properties

Document properties are attributes that determine what users see on the document property sheets when they create DMS documents. In the GroupWise Windows client, the default document properties for a new document appear like this:

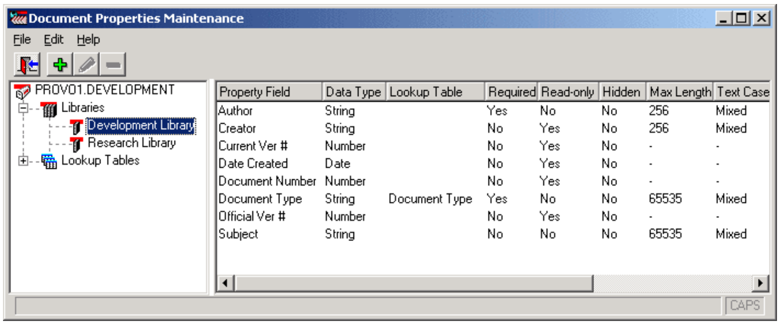


Library:	Development Library
Document number:	
Subject:	
Document type:	Document
Author:	Harry Wong
Creator:	
Date created:	06/11/01 10:31AM
Official version:	0
Current version:	

□ Open document now

NOTE: In the Cross-Platform client, you cannot create new documents in GroupWise.

In ConsoleOne, the default document properties for a library are defined like this:



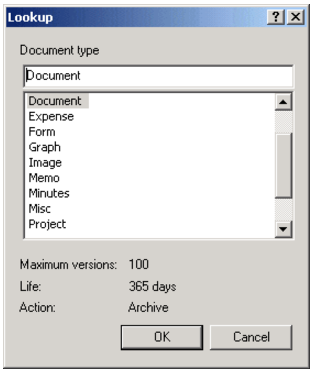
Property Field	Data Type	Lookup Table	Required	Read-only	Hidden	Max Length	Text Case
Author	String		Yes	No	No	256	Mixed
Creator	String		No	Yes	No	256	Mixed
Current Ver #	Number		No	Yes	No	-	-
Date Created	Date		No	Yes	No	-	-
Document Number	Number		No	Yes	No	-	-
Document Type	String	Document Type	Yes	No	No	65535	Mixed
Official Ver #	Number		No	Yes	No	-	-
Subject	String		No	No	No	65535	Mixed

The default document properties are often adequate, but for some libraries, additional customized document properties can be very useful. For example, the legal department might want Client and Matter fields to be required for most documents created by anyone in that department.

NOTE: Document properties cannot be set in ConsoleOne on Linux. However, you can use ConsoleOne on Windows to set document properties for libraries that are located on Linux.

Document Types

The Document Type property defines how a document is disposed of when its "life" in the system has expired. It is a required field. Users select a document type each time they create a new document.



Document type: Document

Maximum versions: 100
Life: 365 days
Action: Archive

A number of default document types are provided, as shown above. If needed, you can set up additional document types. For example, you could set up Pleading for the legal department, Spreadsheet for accounting, Correspondence for administration, RFP for marketing, White Paper for R&D, and so on.

The document type establishes the following document characteristics:

- "Maximum Versions" on page 267
- "Expiration Actions" on page 268
- "Document Life" on page 268

The following table lists some of the default document types and their default characteristics:

Document Type	Maximum Versions	Expiration Action	Document Life
Agenda	100	Archive	99 days
Document	100	Archive	365 days
Memo	1	Delete	99 days
Minutes	100	Archive	99 days
Misc	10	Archive	30 days
Proposal	100	Archive	99 days
Report	100	Archive	99 days
Template	100	Archive	365 days

Maximum Versions

Users can create new versions of their documents when they revise them. Version numbers are automatically incremented.

Any version of a document can be designated as the official version by the user. The official version, which is not necessarily the most recently-edited version, is the one located in searches. GroupWise users have the right to designate an official version if they have Edit rights to the document.

Each document type property has a maximum number of versions (up to 50,000 per document). Most types have a default of 99 versions. A maximum of 0 (zero) versions means that documents of that type cannot have versions.

Document Life

Document life is the number of days that must pass between the time when a document is last accessed and when it is ready for archival or deletion. A document life value of 0 (zero) indicates that the document will never be available for archival or deletion.

Expiration Actions

When a document's life expires, its associated expiration action takes place:

Archive: The document will be archived when it reaches its document life date. This is useful for important documents because archived documents can be unarchived.

Delete: The document will be automatically deleted when its document life date is reached. This is useful for documents that are temporary in nature.

Retain: The document will not be deleted or archived, and will remain in the system indefinitely. This option is practical for documents that have a recurring use, such as template documents.

Integrations

Integrations serve as the "glue" between document-producing applications and your GroupWise DMS system. Integrations provide code specifically designed to allow function calls, such as Open or Save, to be redirected to the GroupWise Windows client. This allows GroupWise dialog boxes to be displayed instead of the application's normal dialog boxes for the integrated functions. Integrations also allow GroupWise to pull documents from a library and deliver them to applications for modification. Then, integrations enable GroupWise to return modified documents to the library so that other users can access them.

NOTE: The Cross-Platform client does not include integrations, which is why you cannot create and edit documents from the Cross-Platform client.

For complete information on the integrations available for the Windows client, see Chapter 24, "Integrations," on page 331.

22 Creating and Managing Libraries

When you first set up a new GroupWise® system, a basic library is automatically created for the first post office. A basic library is adequate when:

- Document management is not a primary activity of your GroupWise users.
- The library will store documents created and used by members of the post office that owns the library, or, if you do not need one basic library per post office, by all users within a domain.
- All documents will be stored at the post office or in a single document storage area external to the post office that owns the library.

If your anticipated document management needs are more demanding than those listed above, you can set up one or more full-service libraries, where you can implement the full range of document management capabilities offered by GroupWise Document Management Services (DMS).

NOTE: The Linux version of ConsoleOne allows you to create libraries, but it does not allow you to set document properties as described in "Organizing Documents" on page 306. As you plan for libraries on Linux, keep in mind that the Cross-Platform client has only basic document management capabilities when compared with the Windows client, as described in "Working with Documents" in the *GroupWise 6.5 Cross-Platform Client User Guide*.

To use one or more libraries as part of your GroupWise system, perform the following tasks as needed:

- "Planning a Basic Library" on page 269
- "Setting Up a Basic Library" on page 272
- "Planning Full-Service Libraries" on page 273
- "Setting Up a Full-Service Library" on page 284
- "Managing Libraries" on page 288
- "Library Worksheets" on page 300

IMPORTANT: If you are creating a new library in a clustered GroupWise system, see the appropriate section of the GroupWise 6.5 Interoperability Guide before you create the library

- "Planning a New Library for a Clustered Post Office" in "Novell Cluster Services"
- "Planning a Library for a New Clustered Post Office" in "Microsoft Clustering Services"

Planning a Basic Library

An initial basic library was created along with the first post office when you set up your GroupWise system. That initial basic library is available for immediate use. However, you might want to change the location where documents are stored, as described in "Deciding Where to Store Documents" on page 271. You can also create additional basic libraries as needed.

This section provides the information you need in order to set up a new basic library. The "Basic Library Worksheet" on page 300 lists all the information you need as you set up a basic library. You should print the worksheet and fill it out as you complete the tasks listed below:

- "Selecting the Post Office That the Library Will Belong To" on page 270
- "Determining the Context for the Library Object" on page 270
- "Choosing the Library Name" on page 270
- "Deciding Where to Store Documents" on page 271

After you have completed the tasks and filled out the worksheet, you are ready to continue with "Setting Up a Basic Library" on page 272.

Selecting the Post Office That the Library Will Belong To

If you are creating a basic library for each post office in your GroupWise system, print a copy of the "Basic Library Worksheet" on page 300 for each post office.

If users in several post offices will store documents in the same basic library, you must decide which post office should own the library. A library can never be reassigned to a different post office, so you should choose the owning post office carefully. You should consider which users will use the library most frequently and where you might want to create additional libraries in the future.

BASIC LIBRARY WORKSHEET
Under Item 3: Post Office, specify the name of the post office that will own the new basic library.

Determining the Context for the Library Object

Generally, you should create the Library object in the same context as its post office. You cannot move a Library object after you have created it.

BASIC LIBRARY WORKSHEET
Under Item 1: eDirectory Container, specify the container for the Library object.

Choosing the Library Name

When you create the Library object, you must give the library a name. This is the name that is displayed in ConsoleOne®.

After you have specified the library's name and created the Library object, the name cannot be changed. Therefore, if you have or will have other libraries, you should pick a name that uniquely identifies the library. For example, use the name to identify the post office it is assigned to.

Do not use any of the following characters in the library's name:

ASCII characters 0-13	Comma ,
Asterisk *	Double quote "
At sign @	Extended characters
Braces { }	Parentheses ( )
Colon :	Period .

By default, the library name that users see in the GroupWise client is the same as the Library object name. However, you can change the display name if you want it to be different from the Library object name.

BASIC LIBRARY WORKSHEET

Under Item 2: Library Name, specify the Library object name.

Under Item 7: Library Description, provide a brief description of the planned use for the library.

Under Item 8: Display Name, specify the library name you want users to see in the GroupWise client, if it is different from the Library object name.

Deciding Where to Store Documents

You can store documents at the post office in the *post_office*\gwdms\library\docs subdirectory of the post office. You can later add document storage areas outside the post office if DMS usage grows. However, the documents stored at the post office can never be moved.

A document storage area has the same internal directory structure that is used to store documents at the post office, but it can be located anywhere in your system. Document storage areas can be moved easily, so it is easy to expand your document storage capacity when you store documents in document storage areas rather than at the post office.

You might want to set up a document storage area on the same server where the POA runs so as not to increase network traffic. The POA can index and serve documents to users most efficiently if the document storage area is located locally.

BASIC LIBRARY WORKSHEET

Under Item 4: Store Documents at the Post Office?, mark Yes or No. (No is recommended for permanent document storage).

To define a document storage area, you must know its direct access path. For example, a UNC path specifies the absolute location of the document storage directory.

Syntax:
\\NetWare_server\volume\storage_directory
\\Windows_server\sharename\storage_directory

Example:

```
\\nw6\gwdocs\docs
\\win2k\c$\docs
```

NOTE: On Linux, ConsoleOne interprets a UNC path so that the first item in the UNC path is the Linux server hostname, followed by a Linux path to the document storage area.

BASIC LIBRARY WORKSHEET

If you entered No for Item 4, specify the direct access path under Item 6: Document Storage Area Path.

Under Item 5: Document Storage Area Description, enter a useful description of the document storage area. (This description is displayed only in ConsoleOne.)

If you need to add a document storage area to the initial library that was created with the first post office in your GroupWise system, use the Storage Areas properties page of the Library object in ConsoleOne to provide the direct access path, as described in "Adding a Document Storage Area" on page 290.

Setting Up a Basic Library

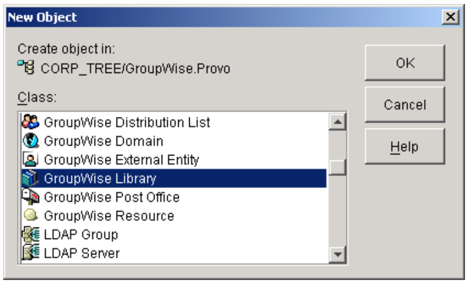
You should already have reviewed "Planning a Basic Library" on page 269 and filled out the "Basic Library Worksheet" on page 300. Complete the following tasks to set up a new basic library:

- "Creating the Basic Library" on page 272
- "Viewing a New Library in Your GroupWise System" on page 287

Creating the Basic Library

To create a new library:

1. Make sure the POA is running for the post office that will own the new basic library.
2. In ConsoleOne, browse to and right-click the Novell® eDirectory™ container where you want to create the library (worksheet item 1), then click New > Object.

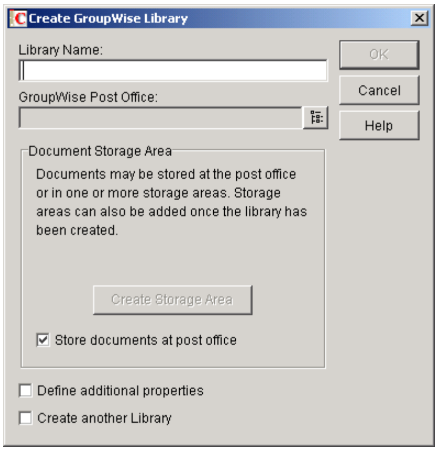


New Object

Create object in:
CORP_TREE/GroupWise.Provo

Class:
- GroupWise Distribution List
- GroupWise Domain
- GroupWise External Entity
- GroupWise Library
- GroupWise Post Office
- GroupWise Resource
- LDAP Group
- LDAP Server

3. Double-click GroupWise Library, then fill in the fields in the Create GroupWise Library dialog box (worksheet items 2 through 6).



Create GroupWise Library

Library Name:

GroupWise Post Office:

Document Storage Area

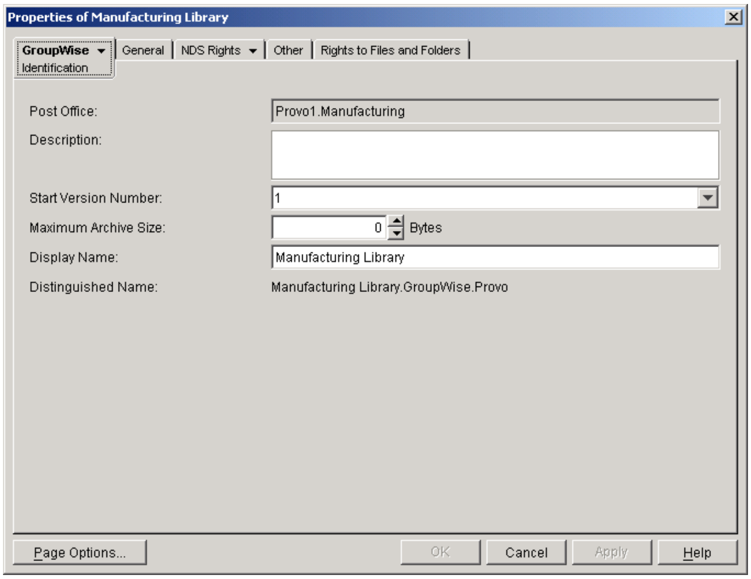
Documents may be stored at the post office or in one or more storage areas. Storage areas can also be added once the library has been created.

☑ Store documents at post office

☐ Define additional properties

☐ Create another Library

4. Click Define Additional Properties, then click OK to create the Library object and display the library Identification page.



Post Office: Provo1.Manufacturing

Description:

Start Version Number: 1

Maximum Archive Size: 0 Bytes

Display Name: Manufacturing Library

Distinguished Name: Manufacturing Library.GroupWise.Provo

5 Fill in the Description field (worksheet item 7).

6 If necessary, edit the Display Name field (worksheet item 8).

7 Click OK to save the library information.

8 Test the new library. See "Viewing a New Library in Your GroupWise System" on page 287.

Although there are many configuration options for libraries and documents, as described in "Planning Full-Service Libraries" on page 273, no additional setup is required for a basic library. GroupWise client users can begin to store documents in the new library at once.

Planning Full-Service Libraries

If your document management requirements go beyond basic libraries, you can create one or more full-service libraries. You might or might not need to make use of all document management features in order to meet your DMS users' needs.

This section covers everything you should consider when you set up full-service libraries. The "Full-Service Library Worksheet" on page 301 lists all the information you need as you set up a full-service library. You should print a copy of the worksheet for each library you plan to create. Fill out the worksheet for each library as you complete the tasks listed below.

- "Deciding Which Libraries to Create" on page 274
- "Selecting the Post Offices That Will Own Libraries" on page 278
- "Determining the Contexts for Library Objects" on page 278
- "Choosing Library Names" on page 278
- "Deciding Where to Store Documents" on page 279
- "Setting Document Version Options" on page 281
- "Figuring Maximum Archive Directory Size" on page 281
- "Designating Initial Librarians" on page 282
- "Restricting Initial Public Library Rights" on page 283

- "Determining Your Indexing Needs" on page 284
- "Determining If You Need to Set Up Integrations for DMS Users" on page 284

After you have completed the above tasks and filled out the worksheets, you are ready to continue with "Setting Up a Full-Service Library" on page 284.

Deciding Which Libraries to Create

When designing a system of libraries for your GroupWise system, you should review the following considerations:

- "Library Access for DMS Users" on page 274
- "Centralized vs. Decentralized Library Configurations" on page 274
- "Library Specialization" on page 277

Library Access for DMS Users

Client/server access is the preferred access mode for GroupWise client users. It is the best access mode for DMS users because it enables them to access libraries outside their own post offices.

For information about access modes, see "Post Office Access Mode" on page 422. If some GroupWise users have direct access requirements, see the *GroupWise 5.5 Document Management Services Guide* (http://www.novell.com/documentation/gw55/index.html).

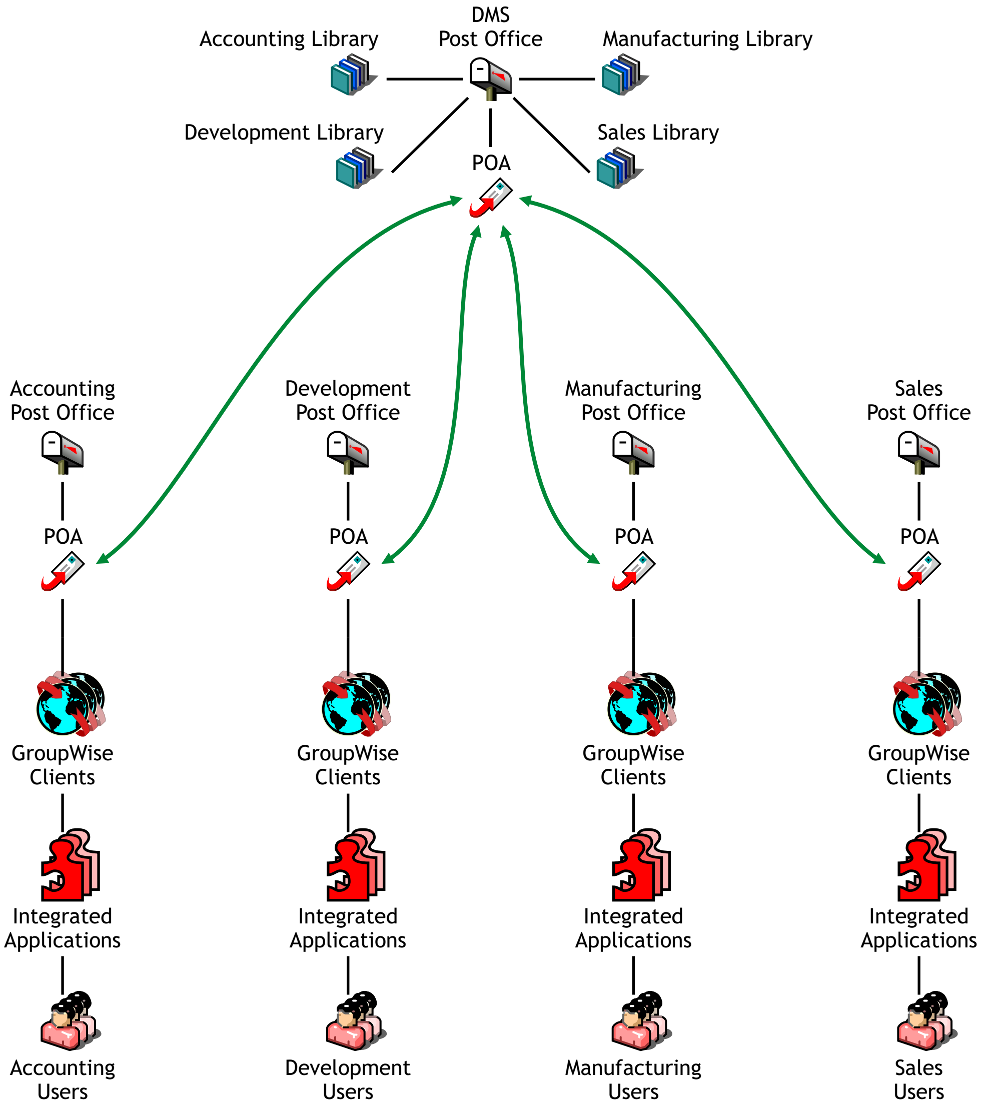
Centralized vs. Decentralized Library Configurations

Reorganizing existing libraries is not a simple process. Therefore, you should determine whether you want a centralized or decentralized library configuration before you start creating libraries.

- "Centralized Libraries" on page 274
- "Decentralized Libraries" on page 276
- "Comparative Scenarios" on page 277

Centralized Libraries

Centralized libraries are located in a post office that is dedicated to libraries (no users). Centralized libraries are serviced by the POA in the dedicated DMS post office, as shown in the following illustration:



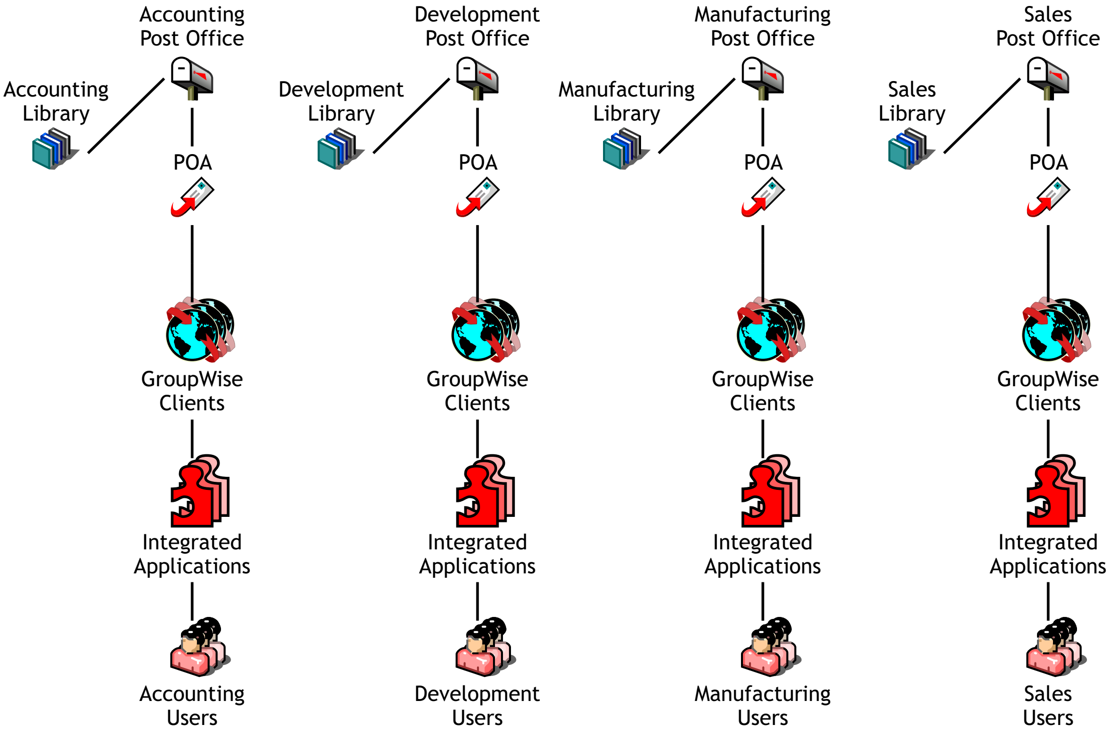
In the illustration, notice that all libraries belong to the DMS post office, which has no users. All GroupWise client users are using client/server access mode, which is required because there are no libraries in their local post offices. Each user has access to all four libraries through TCP/IP links to the DMS POA.

The following table lists some advantages and disadvantages of centralized libraries:

Advantages	Disadvantages
◆ Administration can be consolidated, allowing one administrator to specialize in document management. ◆ Backup can be easier with hardware dedicated to one DMS post office, such as optical drives, RAID, fast backup units, and so on. ◆ If a post office server other than the one dedicated to libraries goes down, DMS access is unaffected for users in the remaining post offices.	◆ You must create and maintain a post office that is dedicated to libraries only (no users). ◆ This configuration guarantees that all document searching and accessing is back and forth between users' post offices and the libraries' post office, possibly degrading network performance. ◆ If the post office server dedicated to libraries goes down, DMS is unusable for the whole GroupWise system.

Decentralized Libraries

Decentralized libraries are located along with users in different post offices. Decentralized libraries are serviced by their own local POAs as shown in the following illustration:



In the illustration, notice that each post office has its own library. Users can see each others' libraries as well as their own because of client/server access mode.

The following table lists some advantages and disadvantages of decentralized libraries

Advantages	Disadvantages
◆ Network traffic is minimized because most document accessing are in users' local post offices. ◆ You do not need to maintain an extra DMS post office dedicated to libraries only. ◆ Users in a post office where a library resides can use direct access mode if necessary.	◆ Libraries and their documents are scattered over different servers, adding to your administrative workload (such as doing backups).

Comparative Scenarios

The following scenarios further illustrate the differences between centralized and decentralized libraries:

- Assume that you assigned your first library to the same post office your users have membership in. By initially assigning a library to the same post office as your users, you establish a decentralized configuration for future libraries. You now want a centralized library configuration. However, because you cannot reassign the library to another post office, you must do one of the following:
  - Create one or more new libraries under a DMS post office, export all of the documents from the first library and import them to the new libraries, delete the first library, and then ensure that users can locate their documents.
  - Create one or more new libraries under a DMS post office and have your librarian use mass document operations to move the documents from the first library to the other libraries, delete the first library, and then ensure that users can locate their documents.
- Assume that you assigned your first library to a DMS post office that is used only for libraries. Now you can use either the centralized or decentralized library configuration for your additional libraries. The DMS post office can be used for all future libraries to create a centralized configuration, or you could assign future libraries to other post offices and leave that first one where it is, giving you a decentralized configuration. Setting up your first library on a post office server dedicated to only libraries allows you to use either configuration option. However, this method initially requires additional hardware and administration.

Library Specialization

You can create libraries for such user specialties as administration, accounting, development, human resources, legal, marketing, manufacturing, payroll, R&D, sales, shipping, and so on. You can also specialize libraries by such functions as general (for all users), administration (including legal and payroll), engineering and documentation development (R&D), marketing and sales, manufacturing and shipping, and so on.

You can also use specialization to provide security for sensitive libraries. You do this by setting up access restrictions for the libraries. The default is for all DMS users to have access to all libraries in the GroupWise system. For more information about restricting library access, see "Managing Library Access" on page 293.

Restricting library access can also improve users' search time. When users install the GroupWise client on their workstations, they are either automatically assigned a default library (if there is one on their post office), or they are asked to select one from the libraries they have access to. By default, DMS searches are performed only on the user’s default library. To search other libraries ("global" search), users can select other libraries using the Look In list in the Find dialog box. If you limit users’ access to libraries (perhaps by department), their global searches would also be faster.

Another reason for creating specialized libraries could be for different library configuration needs. For example, each library could have specialized document types and document properties that would not be needed in other libraries. For a review of document types and properties, see “Documents” on page 265. For more detailed information, see “Customizing the Default Document Type Property” on page 307 and “Customizing Document Properties” on page 306.

Specialization can also facilitate library management activities, such as controlling library accessibility for individual users or groups of users, or managing different uses of document types, document properties, or field label naming schemes.

Selecting the Post Offices That Will Own Libraries

As a result of deciding whether you want to use a centralized or decentralized configuration for your libraries and whether or not you need specialized libraries, you should have a good idea of what post offices you want to create libraries in.

If you are using a centralized configuration, create the DMS post office by following the instructions in Chapter 11, “Creating a New Post Office,” on page 147, then return to this point.

FULL-SERVICE LIBRARY WORKSHEET
Under Item 3: Post Office, specify the name of the post office that will own the new library.

Determining the Contexts for Library Objects

You can create a Library object in any container in the eDirectory tree. For example, you could create the Library object in the same container as its Post Office object. Or you could create it in a special container just for Library objects:

The containers in which you place the Library objects have no bearing on whether your libraries are centralized or decentralized. Library objects can be located anywhere in the tree, no matter which post offices the libraries belong to.

FULL-SERVICE LIBRARY WORKSHEET
Under Item 1: eDirectory Container, specify the name of the eDirectory container where you want to create the new library.

Choosing Library Names

A library’s name must be unique within the post office; it also must be unique within its container. You should devise a naming scheme that will help to identify all libraries in the GroupWise system. It can be useful to include within the library name an indication of which post office it belongs to.

After you have specified the library’s name and created the Library object, the name cannot be changed.

Do not use any of the following characters in the library’s name:

ASCII characters 0-13

Asterisk *

At sign @

Braces { }

Colon :

Comma ,

Double quote "

Extended characters

Parentheses ( )

Period .

By default, the library name that users see in the GroupWise client is the same as the Library object name. However, you can change the display name if you want it to be different from the Library object name.

FULL-SERVICE LIBRARY WORKSHEET

Under Item 2: Library Name, specify the Library object name.

Under Item 7: Library Description, provide a brief description of the planned use for the library.

Under Item 10: Display Name, specify the library name you want users to see in the GroupWise client, if it is different from the Library object name.

Deciding Where to Store Documents

When deciding where to store documents, you should review the following considerations:

- "Document Storage Location" on page 279
- "Disk Space Requirements" on page 279
- "Direct Access Paths to Document Storage Areas" on page 280

Document Storage Location

Documents belonging to full-service libraries should *not* be stored at the post office. Instead, they should be stored in document storage areas. For a review, see "Document Storage Areas" on page 265.

A library can have more than one document storage area. The only requirement is that the POA that services the library must have direct network access (mapped drive or mounted file system) to each storage area.

You can set up one document storage area for each library as you create the Library object. Additional document storage areas can be set up using the Storage Areas properties page of the Library object, as described in "Adding a Document Storage Area" on page 290.

Disk Space Requirements

You will need to know the disk space requirements for your libraries in order to choose appropriate locations for document storage areas.

If you have chosen a centralized library configuration, your document storage areas will all be serviced by the POA of the DMS post office. Therefore, you can calculate the disk space requirements for your GroupWise system as a whole. If you have chosen a decentralized configuration, document storage areas will be located throughout your GroupWise system. Therefore, disk space requirements must be calculated separately for each library.

If your current document storage statistics are an accurate indicator for a given library or for your system, use them for calculating your disk space requirements. Otherwise, use the following formula for determining DMS storage needs:

```
   Number of Users
x  Average Number of Documents per User
x  Average Document Size
x  Average Number of Versions per Document
-------------------------------------------
   Disk Space Required for Library
```

Example:

```
   250  Users
x  200  Documents per User
x   50  KB per Document
x   10  Versions per Document
-----------------------
    25  GB of Disk Space
```

Users might create a new version of a document any time they revise it. Because all versions of a document are saved in BLOB storage with the original document, disk space can be used up quickly! If you know how many versions per document your users average, use that value in the formula; otherwise, allow for an average of at least ten versions per document.

If your Average Document Size value for the formula is based on non-GroupWise documents, they will be compressed by about 50% after they have been imported into GroupWise and stored in BLOBs.

You should research your current or expected document usage before deciding where to store documents.

FULL-SERVICE LIBRARY WORKSHEET

Under Item 7: Document Usage Estimate, enter the requested values and calculate the resulting disk space requirements.

If your values are calculated for the system (rather than per library), enter this information on only one of the worksheets.

Direct Access Paths to Document Storage Areas

To define a document storage area, you will need to know its direct access path. For example, a UNC path specifies the absolute location of the document storage directory.

Syntax:
\\NetWare_server\volume\storage_directory
\\Windows_server\sharename\storage_directory

Example:

```
\\nw5\gwdocs\docs
\\win2k\c$\docs
```

NOTE: On Linux, ConsoleOne interprets a UNC path so that the first item in the UNC path is the Linux server hostname, followed by a Linux path to the document storage area.

You might want to set up a document storage area on the same server where the POA runs so as not to increase network traffic. The POA can index and serve documents to users most efficiently if the document storage area is located locally.

FULL-SERVICE LIBRARY WORKSHEET

Under Item 6: Document Storage Area Path, specify the direct access path.

Under Item 5: Document Storage Area Description, provide a useful description of the document storage area. (This description is displayed only in ConsoleOne.)

Setting Document Version Options

When you create a new library, you can establish how document versions are handled. For an overview of document versioning, see "Maximum Versions" on page 267.

- "Official Version" on page 281
- "Start Version Number" on page 281

Restricting the maximum number of versions should be done after the library has been created, as described in "Editing Library Properties" on page 289.

Official Version

By default, any user can establish the official version of a document. However, you can remove that right from one or more users if needed.

FULL-SERVICE LIBRARY WORKSHEET

Under Item 11: Restrict Public Access Rights, cross out Designate Official Version if you want to eliminate that right for all users.

You can later grant the Designate Official Version to specific users or distribution lists, as described in "Managing Library Access" on page 293.

Start Version Number

You must set the start number for each library to either 0 (zero) or 1. The default is 1. This number identifies the original document.

Version numbers are automatically increased from the number you select. If you select 0, the first version of a document will be 000. If you select 1, the first version will be 001.

FULL-SERVICE LIBRARY WORKSHEET

Under Item 8: Start Version Number, select 0 or 1.

Figuring Maximum Archive Directory Size

Documents created with GroupWise DMS can be archived, depending on their Document Type properties. A document's type determines its disposition, such as archiving or deleting. For more information, see "Customizing the Default Document Type Property" on page 307.

When you archive documents, their BLOB files are moved into archive directories. Each library in a document storage area has its own set of archive directories that are automatically created as needed. They are named ar*xxxxxx* (where *xxxxxx* is an incremental integer with leading zeros). A document storage area has the same archive directory structure as the gwdms subdirectory in the post office, as illustrated in "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

When a document is archived, GroupWise determines if the document's BLOB file will fit in the current archive directory. If it will not fit, another archive directory is created and the BLOB is archived there.

An archive set consists of all documents in one archive directory. The Maximum Archive Size property on the Library object establishes in bytes each archive directory's size limit. You should set this to mirror the capacity of your archival medium (such as a CD). It should not be more than your archival medium's capacity.

It is usually better to keep archive sets small in comparison to the size of the backup medium. This lets you back up archive directories often enough to keep your hard disk space from being used up too quickly between backups. For example, if your backup medium has 1 GB capacity, you could limit your archive sets to a maximum archive size of 200 MB.

If your archival system only lets you back up in one pass (in other words, you cannot perform consecutive backups to the medium), the Maximum Archive Size would need to match the archival medium's capacity.

Some archival mediums require extra space for recording file storage data, such as an index of the files stored to tape. Ten percent is usually sufficient. For example, a tape system with 100 MB capacity means you should set your Maximum Archive Size to 90 MB.

Consult your archival medium documentation for information on setting up an effective backup strategy. Include in your strategy such concepts as multiple archive sets per backup medium, or allowing extra space for the medium's file storage data.

ADDITIONAL LIBRARIES WORKSHEET
Under Item 9: Maximum Archive Size, enter a number (in bytes, with no abbreviations or commas).

Designating Initial Librarians

A librarian has full rights to the properties of every document in the library, and can therefore perform management tasks on all library documents. You can assign yourself as a librarian. You can also delegate these tasks by assigning responsible users in each library as librarians. Any GroupWise user who normally has access to the library can be a librarian. You can also have multiple librarians for each library.

When you first create a new library, you might want to simply designate yourself as the librarian and assign other users later. For more detailed information, see "Adding and Training Librarians" on page 295.

ADDITIONAL LIBRARIES WORKSHEET
Under Item 12: Librarians, list any users that you want to function as librarians for the new library.

Restricting Initial Public Library Rights

The rights to documents in a library apply to the library as a whole; therefore, they are referred to as public rights. By default, all public rights are granted to all users in a new library.

You can restrict which GroupWise library features individual users or distribution lists should have by removing the public rights and then restoring them for selected users or distribution lists.

The following table summarizes the public library rights:

Public Right	Description
Add	Allows users to add new documents to the library.
Change	Allows users to make changes to existing documents in the library.
Delete	Allows users to delete documents, regardless of who else created them or has rights to the documents. However, to be able to delete a document, users must also have rights to locate and modify the document (View and Change rights), in addition to the Delete right.
View	By itself, this right allows searching, viewing, or copying documents, but does not permit editing them. Copies can be edited, because a copy is saved as a separate document. Therefore, editing a copy will not affect the original document or any of its versions.
Designate Official Version	Allows any version of a document to be designated as the official version. The official version, which is not necessarily the most recently-edited version, is the one located in searches. The official version is usually determined by the creator or author of the document. However, the official version can be designated by the last user to edit the document (if the user has this right). A user also needs the Change right to the document to be able to designate an official version. However, you might still want to deselect this as an initial public right.
Reset In-Use Flag	The In-Use flag protects against data loss by preventing multiple users from concurrently opening the same document. The purpose of the Reset In-Use Flag right is to allow a user or librarian to reset a document's status when the document is in use by someone else or when it is erroneously flagged as in use. Because you can manually reset the In-Use flag to change a document's status, even if the document is currently open, you should use prudence in allowing users the public right to change the In-Use flag. You might want to deselect this as a public right.

FULL-SERVICE LIBRARY WORKSHEET

Under Item 11: Restrict Public Access Rights, cross out any public rights you want to eliminate for all users.

You can later grant the rights to specified users or groups, as described in "Managing Library Access" on page 293.

Rights to individual documents in a library can be modified at any time by the user listed as the creator or author of the document. Just because users might have public rights in a library does not mean that they will have the equivalent rights to every document in the library. For additional information on rights, see "Sharing Documents" in "Creating and Working with Documents" in the *GroupWise 6.5 Windows Client User Guide*.

Determining Your Indexing Needs

The POA performs many tasks in the post offices, as described in "Role of the Post Office Agent" on page 423. Indexing documents is just one of its many functions.

If necessary, you can configure an extra POA on another server to handle indexing. Separating POA functions can optimize the processing load for the respective POAs, particularly if your GroupWise system will regularly search and index a large number of documents.

If you feel you might need dedicated indexing for DMS documents, see "Indexing Documents" on page 319 for in-depth information on different configurations. Then determine whether you will need dedicated indexing.

FULL-SERVICE LIBRARY WORKSHEET

Under Item 11: Dedicated POA for Indexing, mark whether or not you plan to set up a separate indexing POA.

Determining If You Need to Set Up Integrations for DMS Users

For an overview of integrations, see "Integrations" on page 268. To determine if you will need to set up integrations for a given application, see Chapter 24, "Integrations," on page 331.

NOTE: This item does not apply if all of your users use the Cross-Platform client, where integrations are not available.

ADDITIONAL LIBRARIES WORKSHEET

Under Item 14: Set Up Integrations, mark whether or not you need to manually set up integrated applications for your DMS users.

Setting Up a Full-Service Library

You should have already reviewed "Planning Full-Service Libraries" on page 273 and filled out the "Full-Service Library Worksheet" on page 301 for each new library. Before starting to create new libraries, be sure your system meets the following prerequisites:

- Make sure the eDirectory contexts exist where you will create new Library objects.
- Make sure the post offices exist that will own the new libraries. If you are using a centralized configuration, make sure you have created the DMS post office that will own all the libraries by following the instructions in Chapter 11, "Creating a New Post Office," on page 147.
- Make sure the POA is running for each post office that will own a new library.
- Make sure you have access to the physical locations where you will set up document storage areas.

After the prerequisites are met, you are ready set up one or more full-service libraries.

- "Creating the Full-Service Library" on page 285
- "Viewing a New Library in Your GroupWise System" on page 287
- "Other Things You Can Do" on page 287

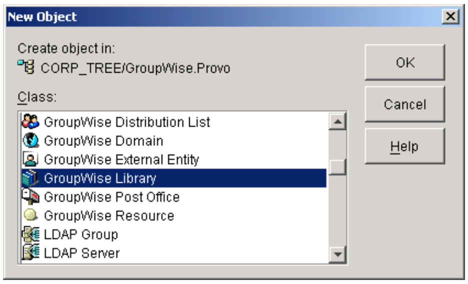
Creating the Full-Service Library

To create a new library:

1 Make sure you are logged in to the eDirectory tree where you want to create the library.

This must be the same tree as the post office the library will belong to (worksheet item 3).

2 In ConsoleOne, browse to and right-click the eDirectory container where you want to create the library (worksheet item 1), then click New > Object.

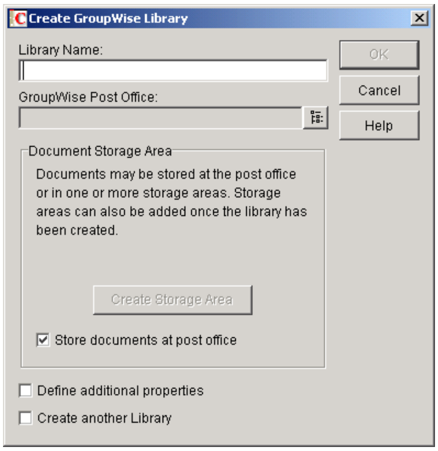


New Object

Create object in:
CORP_TREE/GroupWise.Provo

Class: GroupWise Library

3 Double-click GroupWise Library, then fill in the fields in the New Library dialog box (worksheet items 2 through 6).



Create GroupWise Library

Library Name:

GroupWise Post Office:

Document Storage Area

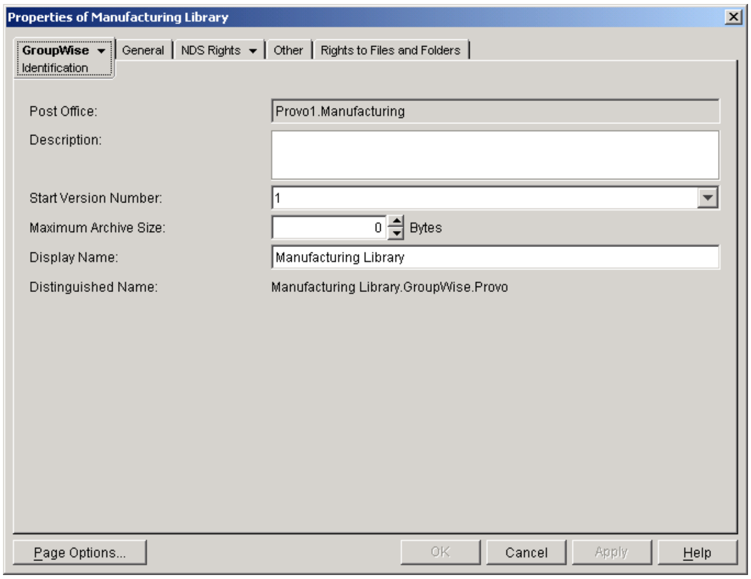
Documents may be stored at the post office or in one or more storage areas. Storage areas can also be added once the library has been created.

☑ Store documents at post office

□ Define additional properties

□ Create another Library

4 Click Define Additional Properties, then click OK to create the new Library object and display the library Identification page.



Post Office: Provo1.Manufacturing

Description:

Start Version Number: 1

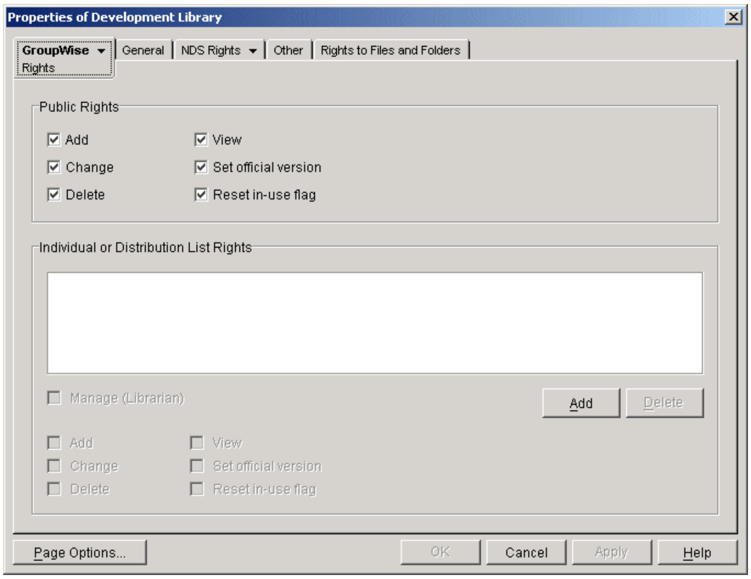
Maximum Archive Size: 0 Bytes

Display Name: Manufacturing Library

Distinguished Name: Manufacturing Library.GroupWise.Provo

5 Fill in the fields (worksheet items 7 through 10).

6 Click GroupWise > Rights to display the Rights page.



Public Rights

☑ Add ☑ View

☑ Change ☑ Set official version

☑ Delete ☑ Reset in-use flag

Individual or Distribution List Rights

□ Manage (Librarian)

□ Add □ View

□ Change □ Set official version

□ Delete □ Reset in-use flag

7 In the Public Rights box, deselect any rights you want to remove from all library users (worksheet item 11).

8 If you want to set up one or more librarians, click Add, browse to and select one or more users or distribution lists (worksheet item 12), then click OK. Select the users and distribution lists, then select Manage (Librarian) to give them rights to the properties of all documents in the library.

9 Click OK to save the library information.

10 Test the library. See "Viewing a New Library in Your GroupWise System" on page 287

Other Things You Can Do

After you have created the new library, you can expand its capabilities as needed:

- Import and manage documents. See Chapter 23, “Creating and Managing Documents,” on page 303
- Set up integrated applications for DMS users (worksheet item 14). See Chapter 24, “Integrations,” on page 331
- Grant library rights to specific users or distribution lists. See “Managing Library Access” on page 293.
- Assign librarians. See “Adding and Training Librarians” on page 295.
- Set up multiple document storage areas. See “Adding a Document Storage Area” on page 290.
- Set up a dedicated indexing POA (worksheet item 13). See “Indexing Documents” on page 319

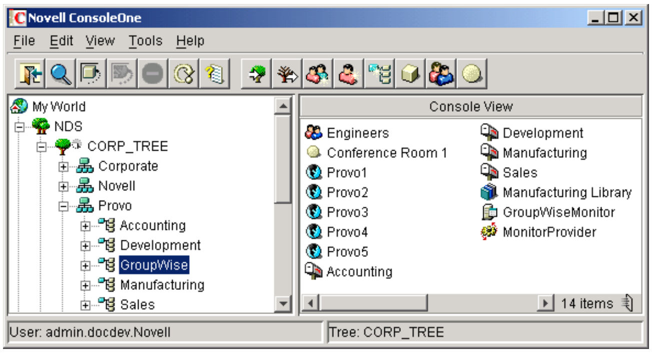
Viewing a New Library in Your GroupWise System

After you create a new library, you can see it in ConsoleOne and GroupWise client users can see it in the GroupWise client.

- “Seeing the New Library in ConsoleOne” on page 287
- “Seeing the New Library in the GroupWise Windows Client” on page 288

Seeing the New Library in ConsoleOne

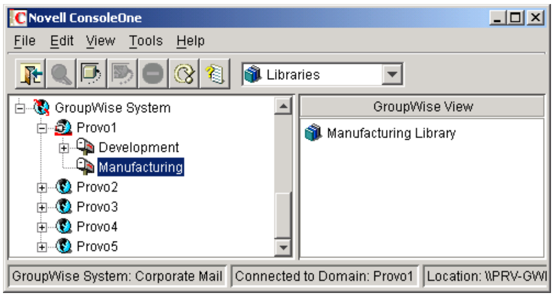
In the Console View in ConsoleOne, you can see the new Library object in the context of its eDirectory container object.



In the GroupWise View, you can see the relationship between the new library and the post office it belongs to.

To locate the library in the GroupWise view:

1. Expand the GroupWise System object.
2. Expand the Domain object where the owning post office resides.
3. Select the owning post office.
4. In the drop-down list of objects, select Libraries.



GroupWise System
Provo1
Development
Manufacturing
Provo2
Provo3
Provo4
Provo5

Manufacturing Library

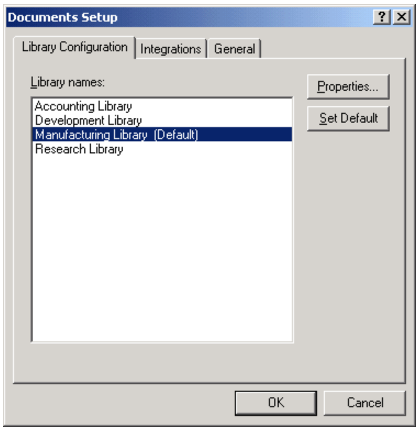
GroupWise System: Corporate Mail | Connected to Domain: Provo1 | Location: \\PRV-GWI

Seeing the New Library in the GroupWise Windows Client

GroupWise Windows client users can see that a new library has been created. They can set it as their default library if desired.

In the GroupWise client:

1 Click Tools > Options > Documents.



Library names:
Accounting Library
Development Library
Manufacturing Library (Default)
Research Library

The Library Configuration tab should include the new library.

2 Select the new library, click Set as Default, then click OK to use the new library as the default location for storing documents and searching for documents.

Managing Libraries

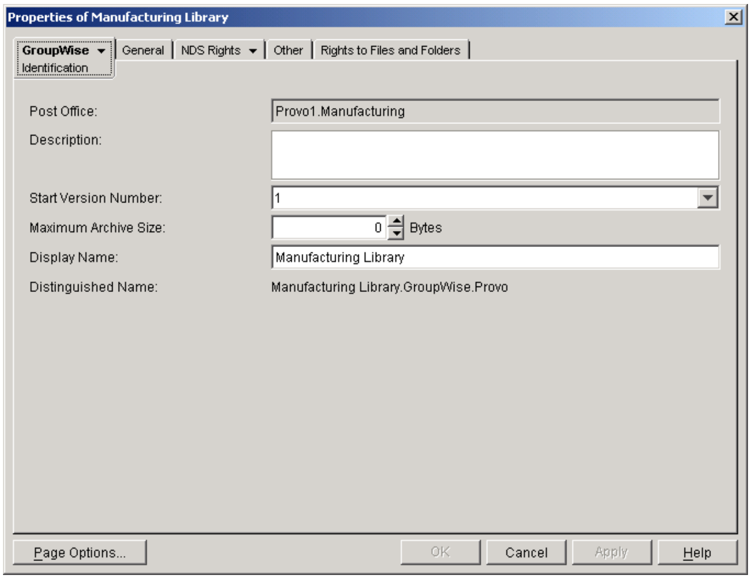
As your GroupWise DMS system grows and evolves, you might need to perform the following activities:

- "Editing Library Properties" on page 289
- "Managing Document Storage Areas" on page 290
- "Managing Library Access" on page 293
- "Adding and Training Librarians" on page 295
- "Maintaining Library Databases" on page 299
- "Moving a Library" on page 299
- "Deleting a Library" on page 299

Editing Library Properties

After creating a library, you can change some library properties. Other library properties cannot be changed.

1 In ConsoleOne, browse to and right-click the Library object, then click Properties to display the library Identification page.



Post Office: Provo1.Manufacturing

Description:

Start Version Number: 1

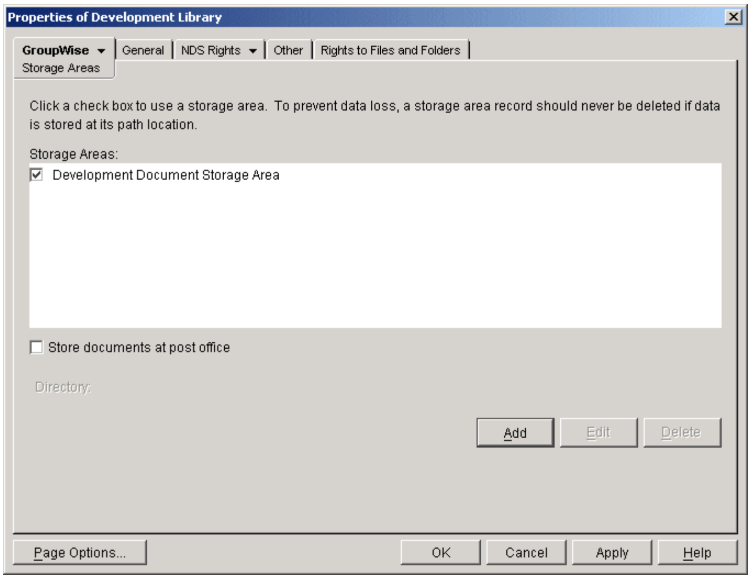
Maximum Archive Size: 0 Bytes

Display Name: Manufacturing Library

Distinguished Name: Manufacturing Library.GroupWise.Provo

2 Change editable fields as needed. For information about individual fields, click Help.

3 Click GroupWise > Storage Areas to display the Storage Areas page.



Click a check box to use a storage area. To prevent data loss, a storage area record should never be deleted if data is stored at its path location.

Storage Areas:

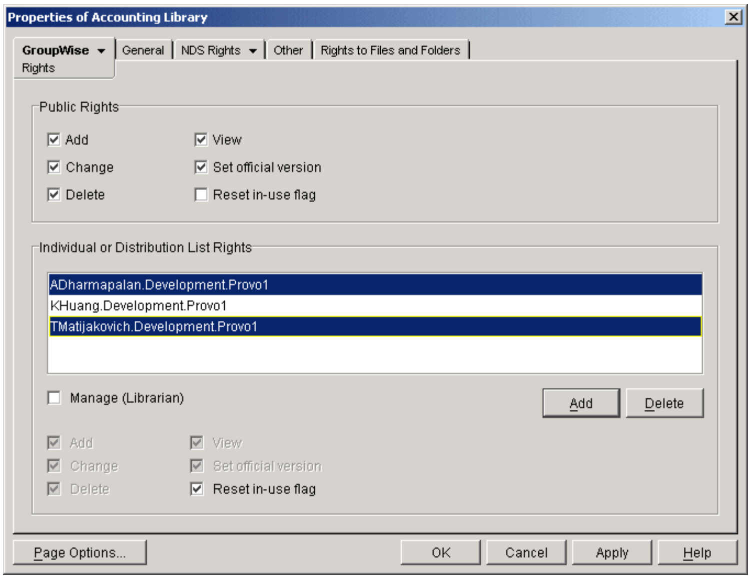
☑ Development Document Storage Area

□ Store documents at post office

Directory:

All document storage areas associated with the library are listed, no matter where they are located. On this page, you can add, move, and delete document storage areas. See "Managing Document Storage Areas" on page 290.

4 Click GroupWise > Rights to display the library Rights page.



Public Rights

☑ Add ☑ View

☑ Change ☑ Set official version

☑ Delete □ Reset in-use flag

Individual or Distribution List Rights

ADharmapalan.Development.Provo1

KHuang.Development.Provo1

TMatijakovich.Development.Provo1

□ Manage (Librarian)

☑ Add ☑ View

☑ Change ☑ Set official version

☑ Delete ☑ Reset in-use flag

Public library rights granted to all users are selected in the Public Rights box. The Individual and Distribution List Rights box shows any additional rights that have been granted to specific users. See "Managing Library Access" on page 293 and "Adding and Training Librarians" on page 295.

5 Click OK to save changes to the library properties.

Managing Document Storage Areas

For a review, see "Document Storage Areas" on page 265 and "Deciding Where to Store Documents" on page 271.

Typically, the initial document storage area for a library is set up when the library is created. Thereafter, you can create additional document storage areas as the library grows. You can move a document storage area to a location where more storage is available. You can delete a document storage area if it is no longer used.

- "Adding a Document Storage Area" on page 290
- "Moving a Document Storage Area" on page 292
- "Deleting a Document Storage Area" on page 292

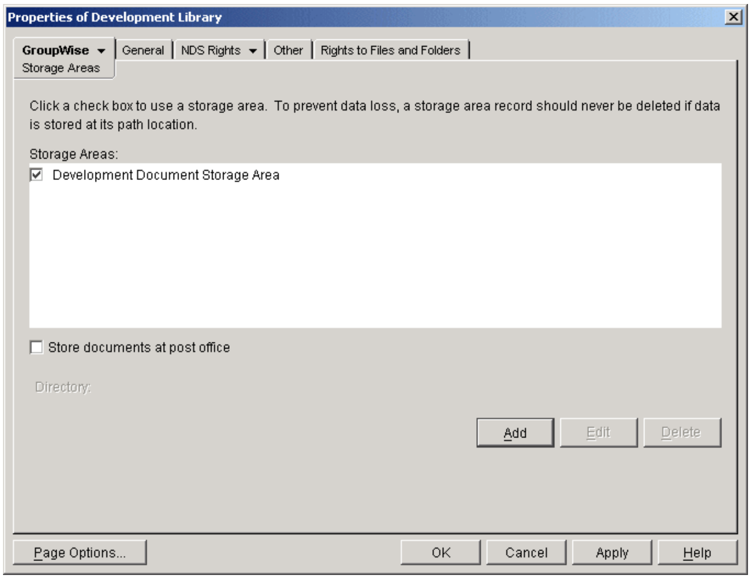
Adding a Document Storage Area

To help you plan where to create the new document storage area, see "Deciding Where to Store Documents" on page 271.

To create a new document storage area for a library:

1 In ConsoleOne, browse to and right-click the Library object, then click Properties.

2 Click GroupWise > Storage Areas to display the Storage Areas page.



Click a check box to use a storage area. To prevent data loss, a storage area record should never be deleted if data is stored at its path location.

Storage Areas:

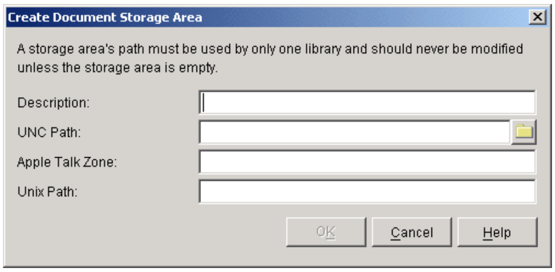
☑ Development Document Storage Area

□ Store documents at post office

Directory:

Existing document storage areas are listed.

3 Click Add to create a new document storage area.



A storage area's path must be used by only one library and should never be modified unless the storage area is empty.

Description:

UNC Path:

Apple Talk Zone:

Unix Path:

4 Provide a description for the document storage area.

5 Specify the UNC path to the directory where you want to create the document storage area.

If the directory does not exist, it will be created as the document storage area is set up.

As an alternative, you can specify an AppleTalk zone to store documents on an Apple* computer, or you can specify a UNIX path to store documents on a UNIX server. On Linux, you can specify a Linux path. The POA that will service the library must have direct access to the location you specify.

6 Click OK to create the new document storage area and add it to the list of storage areas for the library.

If you have multiple document storage areas selected in the Storage Areas list, new and modified documents could be added to any one of them.

7 If you want to stop storing documents in the previous document storage area, deselect it in the Storage Areas list.

8 Click OK to save the document storage area information.

Moving a Document Storage Area

You might choose to move a document storage area if it is close to exceeding the available disk space at its current location and you do not want to create an additional document storage area.

To move a document storage area:

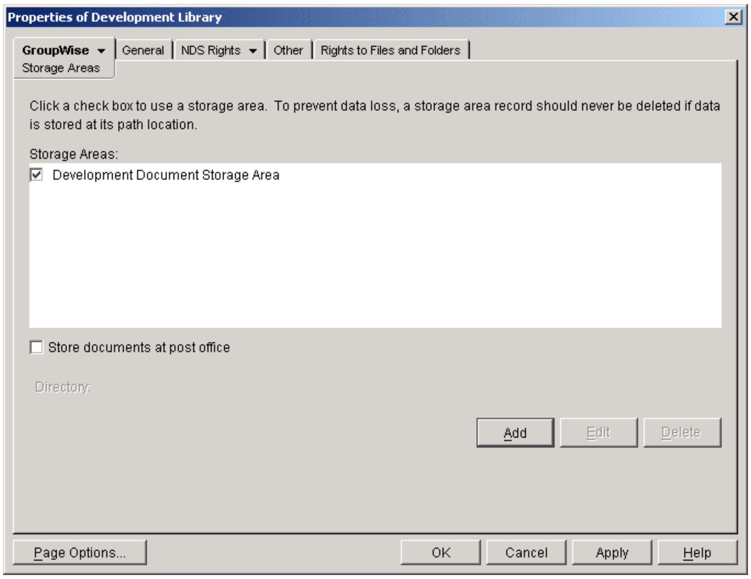
1 Stop the POA that services the library. See "Stopping the POA" on page 480.

2 Copy the document storage area directory and all of its contents to the desired location.

3 Make sure that the POA will have access to the new location so that it can read and write documents in the document storage area.

4 In ConsoleOne, browse to and right-click the Library object, then click Properties.

5 Click GroupWise > Storage Areas to display the Storage Areas page.



Properties of Development Library

Click a check box to use a storage area. To prevent data loss, a storage area record should never be deleted if data is stored at its path location.

Storage Areas:

☑ Development Document Storage Area

□ Store documents at post office

Directory:

Existing document storage areas are listed.

6 Select a document storage area, then click Edit.

7 Provide the new location for the document storage area, then click OK twice to save the new document storage information.

8 Restart the POA. See "Starting the POA" on page 431.

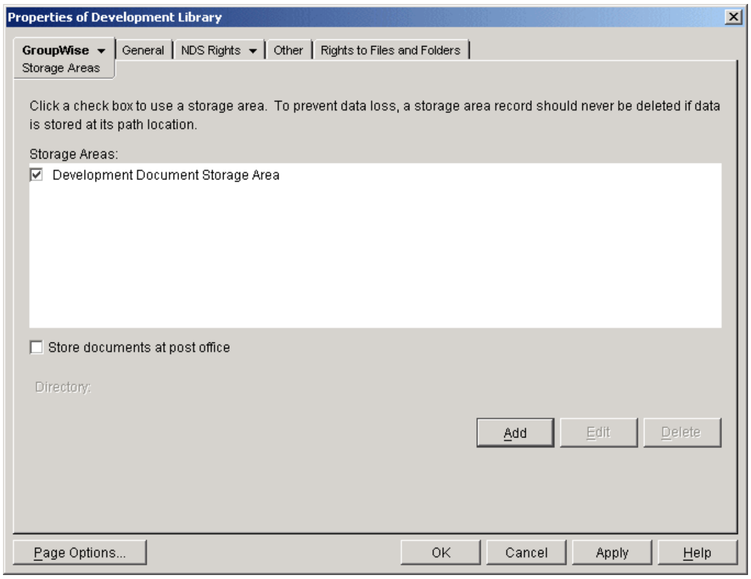
Deleting a Document Storage Area

When you delete a document storage area, any documents in the document storage area are moved to other valid document storage areas for the library. If you want to move documents to a specific location before deleting the document storage area, see "Managing Groups of Documents" on page 305.

To delete a document storage area:

1 In ConsoleOne, browse to and right-click the Library object that owns the document storage area, then click Properties.

2 Click GroupWise > Storage Areas to display the Storage Areas page.



Click a check box to use a storage area. To prevent data loss, a storage area record should never be deleted if data is stored at its path location.

Storage Areas:

☑ Development Document Storage Area

☐ Store documents at post office

Directory:

3 Select a document storage area, then click Delete.

4 Click OK to close the Storage Areas page

If the above steps are not successful in deleting a document storage area, perhaps because one or more documents were in use during the deletion process, you can use the Analyze/Fix Library action of Mailbox/Library Maintenance, with the Remove Deleted Storage Areas and Move Documents First options selected, to finish cleaning up the deleted document storage area. For more information, see Chapter 28, "Maintaining Library Databases and Documents," on page 359.

Managing Library Access

Access to libraries is controlled by the rights users have to the Library object. By default, when a new library is created, all of the following rights are granted:

Public Right	Description
Add	Allows users to add new documents to the library.
Change	Allows users to make changes to existing documents in the library.
Delete	Allows users to delete documents, regardless of who created them or has rights to the documents. However, to be able to delete a document, users must also have rights to locate and modify the document (View and Change rights), in addition to the Delete right.
View	By itself, this right allows searching, viewing, or copying documents, but does not permit editing them. Copies can be edited, because a copy is saved as a separate document. Therefore, editing a copy will not affect the original document or any of its versions.

Public Right	Description
Designate Official Version	Allows any version of a document to be designated as the official version. The official version, which is not necessarily the most recently-edited version, is the one located in searches. The official version is usually determined by the creator or author of the document. However, the official version can be designated by the last user to edit the document (if the user has this right). A user also needs the Change right to the document to be able to designate an official version.
Reset In-Use Flag	The In-Use flag protects against data loss by preventing multiple users from concurrently opening the same document. The purpose of the Reset In-Use Flag right is to allow a user or librarian to reset a document's status when the document is in use by someone else or when it is erroneously flagged as in use. In the GroupWise client the document properties Status field displays the current In-Use flag setting for a document. The Status field is automatically set to In Use when a document is opened and reset to Available when a document is closed. There can also be other values, such as Checked Out. A document cannot be checked out when its status is In Use.

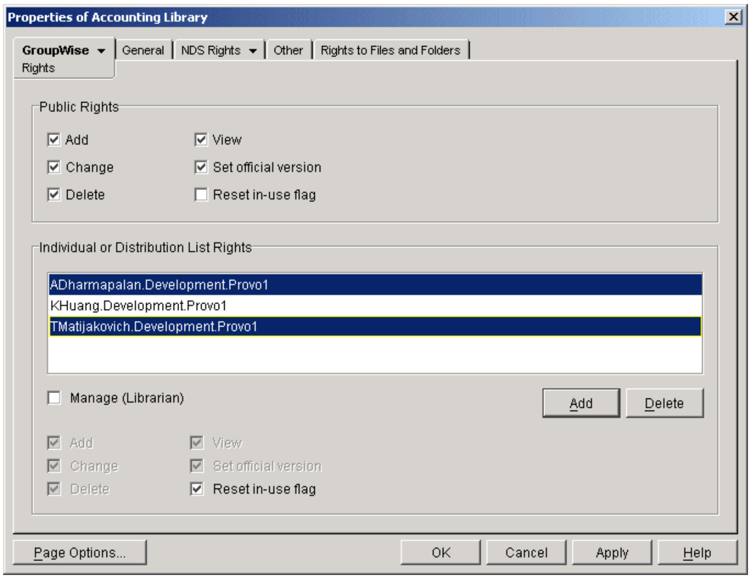
There are a variety of reasons for which you might want to restrict certain library rights, including:

- Your libraries are specialized by department and you want to restrict access to sensitive libraries, such as a payroll library.
- Your libraries are distributed across multiple post offices and you want to restrict the scope of user searches to only the libraries they should use, thereby speeding up searches.
- Your libraries are distributed across multiple servers and you want to minimize network traffic.
- You have some users who should have more rights than other users to certain libraries.

To restrict public rights while granting individual rights:

1. In ConsoleOne, browse to and right-click the Library object, then click Properties.
2. Click GroupWise > Rights to display the Rights page.
3. In the Public Rights box, deselect the rights that you want to remove from all users.
4. Click Add, then browse to and select the users who need to have rights to the library.

   If the number is large, you might find it easier to create a distribution list for users who need rights. Then you can select one distribution list rather than multiple users. See Chapter 18, "Creating and Managing Distribution Lists," on page 239
5. In the Individual or Distribution List Rights box, select the users or distribution lists to grant rights to.
6. Below the list, select the rights that you want to grant.



Public Rights

☑ Add ☑ View
☑ Change ☑ Set official version
☑ Delete □ Reset in-use flag

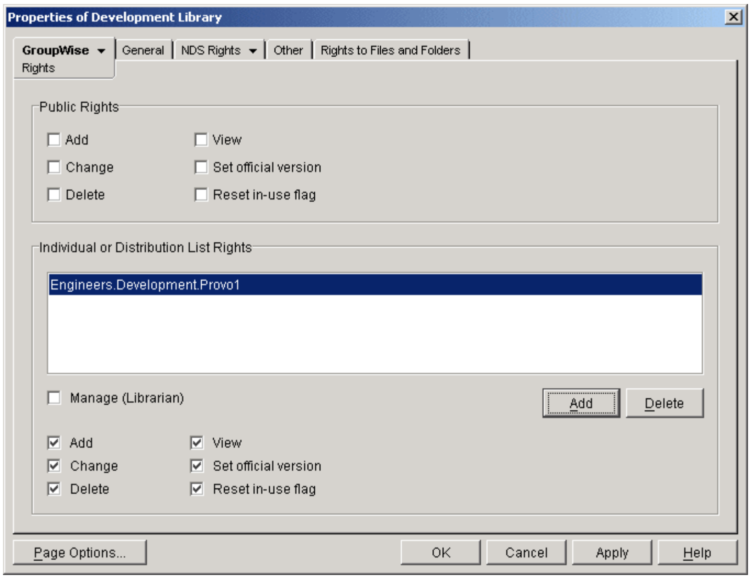
Individual or Distribution List Rights

ADharmapalan.Development.Provo1
KHuang.Development.Provo1
TMatijakovich.Development.Provo1

□ Manage (Librarian)

☑ Add ☑ View
☑ Change ☑ Set official version
☑ Delete ☑ Reset in-use flag

In the first example, only two users are granted the Reset In-Use Flag right.



Public Rights

□ Add □ View
□ Change □ Set official version
□ Delete □ Reset in-use flag

Individual or Distribution List Rights

Engineers.Development.Provo1

□ Manage (Librarian)

☑ Add ☑ View
☑ Change ☑ Set official version
☑ Delete ☑ Reset in-use flag

In the second example, only members of the Engineers group are granted any rights to the Development Library.

7 Click OK to save the updated library rights information.

Adding and Training Librarians

When you first create a library, you might for convenience assign yourself as the initial librarian. As library activity increases you can add librarians, and if desired, remove yourself as a librarian.

- "Understanding the Role of the Librarian" on page 296
- "Setting Up a Librarian GroupWise Account (Optional)" on page 298
- "Assigning Librarians" on page 298

Understanding the Role of the Librarian

Keep in mind the following when assigning librarians:

- "Librarian Identity" on page 296
- "Librarian Functions" on page 296
- "Librarian Rights" on page 297

Librarian Identity

Any GroupWise user with access to a library can be a librarian for the library. You can have multiple librarians for a single library. You can also assign a single user as a librarian for multiple libraries. Because being a librarian entails additional functions and rights in the library, you should choose responsible users as librarians.

Librarian Functions

A librarian can perform the following actions:

- Check out a document without a copy.
- Modify the properties of any document in the library.
- Copy documents to another library.
- Delete both documents and properties.
- Reset a document's status (change the In-Use flag).
- View all activity log records of any document in the library.
- Restore document BLOBs from backup.
- Perform mass operations, such as moving, deleting, archiving, and changing properties.
- Perform searches (but not full-text searches) on documents that are not available for searching by regular users.
- Use GroupWise third-party APIs to generate reports on all library documents.

All operations available to a normal user are also available to a librarian, as long as the security requirement discussed under "Librarian Rights" on page 297 is not compromised. The intention is that librarians will be able to modify their own documents and document properties.

All actions taken by a librarian are written to a document's activity log.

Unless the librarian's own GroupWise user ID is in the Author or Security fields, a librarian *cannot* perform the following functions:

- Open a document
- View a document
- Save a document
- Check out a document with a copy

To help new librarians get started, you should explain these librarian functions to them. You can also refer new librarians to the "librarian users" topic in the GroupWise client help.

Librarian Rights

In addition to the six public rights, libraries also have a Manage right. When you grant the Manage right to a GroupWise user, you designate that user as a librarian. The Manage right gives the librarian full access to the properties of every document in the library. However, the Manage right does *not* grant the librarian direct access to the content of any document.

Because a librarian has full access to document properties, the librarian could add his or her own personal GroupWise user ID to the Author or Security field of a document, thus gaining access to the document's content. However, a high-priority e-mail notification would automatically be sent to the original person listed in the Author field informing him or her of the action by the librarian. Therefore, document privacy is maintained.

The following table lists the various librarian functions, and whether an e-mail notification is sent if the function is performed.

Librarian Function	Notification?
Modify the Author or Security fields	High-priority e-mail to the author
Copy a document	High-priority e-mail to the author
Delete a document	High-priority e-mail to the author
Replace a document with a copy from backup	High-priority e-mail to the author
Perform a mass document operation (copy, move, delete, or archive documents; modify document properties)	Mass operation e-mails
Reset a document's status (In-Use flag)	None
Check out a document without a copy	None
View the activity log of any document	None
Generate reports on any documents (using GroupWise third-party APIs)	None

Note that mass operation notifications do not specify what action was taken by the librarian; they only specify that an action was taken.

The following table lists the document property fields which the librarian has rights to modify, and whether an e-mail notification is sent if the field is modified.

Property Field	Notification?
Subject	No
Author	Yes
Security (sharing list)	Yes
Document Type	No
Version Description	No
Custom Fields	No

Property Field	Notification?
File Extension	No
Official Version	No
Current Version	No

If you remove the Manage right from a user, you will need to manually un-check any rights that the user gained from being made a librarian that the user did not previously have.

Setting Up a Librarian GroupWise Account (Optional)

The Manage right will always be in effect for those users who have been assigned as librarians. However, there might be times librarians will want to act on their own accord without the possibility of seeing or modifying documents that belong to other users.

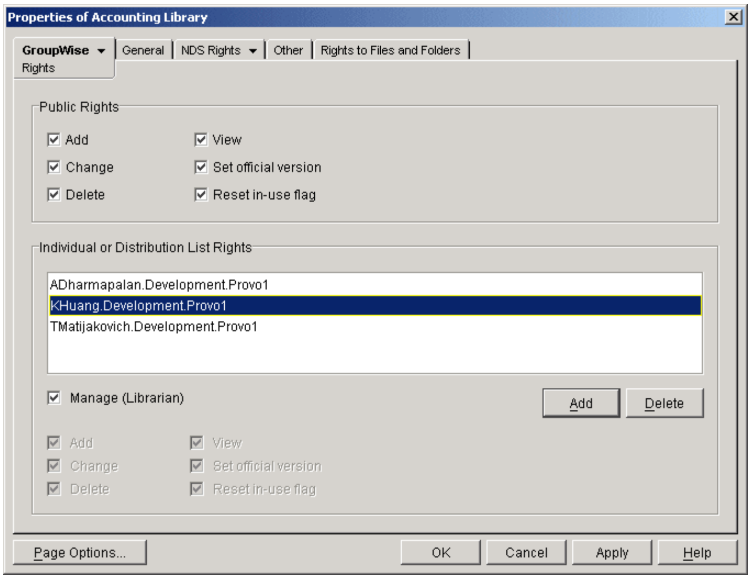
To allow users assigned as librarians to act as normal GroupWise users, you could create a single librarian account for a library and have users who need to perform librarian tasks log in using the librarian GroupWise account and password instead of their own.

If users assigned as librarians log in under a librarian GroupWise account, they will not have access to any documents they would normally have access to under their own accounts, except by altering the Author or Security fields.

Assigning Librarians

To add librarians to a library:

1. In ConsoleOne, browse to and right-click the Library object, then click Properties.
2. Click GroupWise > Rights to display the Rights page.
3. Click Add, browse to and select the users that you want to assign as librarians, then click OK to return to the Rights page.



Public Rights

☑ Add ☑ View
☑ Change ☑ Set official version
☑ Delete ☑ Reset in-use flag

Individual or Distribution List Rights

ADharmapalan.Development.Provo1
KHuang.Development.Provo1
TMatijakovich.Development.Provo1

☑ Manage (Librarian)

☑ Add ☑ View
☑ Change ☑ Set official version
☑ Delete ☑ Reset in-use flag

4. In the Individual or Distribution List Rights box, select the librarian users, select Manage (Librarian), then click OK to save the library rights changes.

Maintaining Library Databases

The Mailbox/Library Maintenance feature of ConsoleOne offers database maintenance features to keep your library and document databases in good condition. See Chapter 28, “Maintaining Library Databases and Documents,” on page 359. It also helps you manage the disk space occupied by library and document databases and document storage areas. See “Reducing the Size of Libraries and Document Storage Areas” on page 371.

When document creators or authors are removed from your GroupWise system, orphaned documents might be left behind. See “Handling Orphaned Documents” on page 329.

To supplement your library maintenance procedures, you should back up your libraries and documents regularly. See “Backing Up a Library and Its Documents” on page 376.

Moving a Library

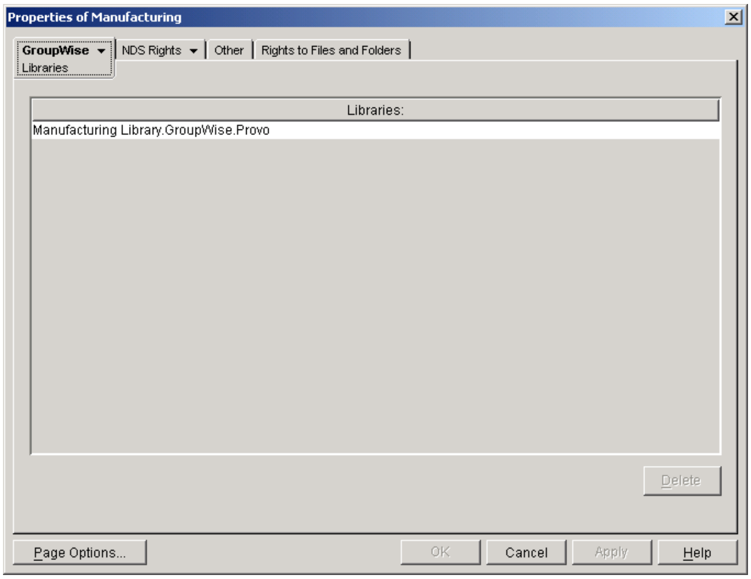
You cannot move a Library object from one location to another in the eDirectory tree. To accomplish the equivalent, you would need to create a new library in the desired location, use a mass move operation in the GroupWise client to move the library’s documents from the old library into the new library, and then delete the old library.

As an alternative to moving the library, you could move just its document storage areas. See “Moving a Document Storage Area” on page 292.

Deleting a Library

You should not delete a library until you make sure that all documents still in the library are no longer needed.

1. In ConsoleOne, browse to and right-click the Post Office object that owns the library to delete, then click Properties.
2. Click GroupWise > Libraries to display the Libraries page.



Libraries:
Manufacturing Library.GroupWise.Provo

3. Select the library to delete, then click Delete.

   All document storages areas and documents are deleted along with the library.

4. Click OK to close the Libraries page and complete the deletion of the library.

Library Worksheets

- "Basic Library Worksheet" on page 300
- "Full-Service Library Worksheet" on page 301

Basic Library Worksheet

For instructions on how to use this worksheet, see "Planning a Basic Library" on page 269.

Item	Explanation
1) eDirectory Container:	Specify the eDirectory container where you will create the Library object. This could be the same container as the post office that the library is assigned to. The Library object cannot later be moved to a different location. For more information, see "Determining the Context for the Library Object" on page 270.
2) Library Name:	Specify a name for the new library. Choose the name carefully. After the library is created, it cannot be renamed. For more information, see "Choosing the Library Name" on page 270.
3) Post Office:	Indicate which post office the library will belong to. A library cannot later be assigned to a different post office. For more information, see "Selecting the Post Office That the Library Will Belong To" on page 270.
4) Store Documents at the Post Office? ◆ No ◆ Yes	Mark No unless you are absolutely certain you will never need to move the documents stored at the post office For more information, see "Deciding Where to Store Documents" on page 271.
5) Document Storage Area Description:	Enter a brief description for the document storage area, including such information as to which post office it belongs, its current capacity in megabytes, and the types of documents that might be stored in it. For more information, see "Deciding Where to Store Documents" on page 271.
6) Document Storage Area Path:	If you are not storing documents at the post office, specify the document storage area for the library. For more information, see "Deciding Where to Store Documents" on page 271.
7) Library Description:	Provide a description for the library to help you identify its function in the system. For more information, see "Choosing the Library Name" on page 270.
8) Display Name:	Specify the library name you want users to see in the GroupWise client, if it is different from the Library object name. For more information, see "Choosing the Library Name" on page 270.

Full-Service Library Worksheet

For instructions on how to use this worksheet, see "Planning Full-Service Libraries" on page 273.

Item	Explanation
1) eDirectory Container:	Specify the name of the eDirectory container where you will create the Library object. This could be the same container as for the post office that owns the library. The LIbrary object cannot later be moved to a different context. For more information, see "Determining the Contexts for Library Objects" on page 278.
2) Library Name:	Specify a name for the new library. Choose the name carefully. After the library is created, it cannot be renamed. For more information, see "Choosing Library Names" on page 278.
3) Post Office:	Specify the post office that the library will belong to. A library cannot later be assigned to a different library. If you will using a centralized library configuration and you have not yet created the DMS post office, follow the instructions in Chapter 11, "Creating a New Post Office," on page 147 before you begin creating libraries. For more information, see "Deciding Which Libraries to Create" on page 274.
4) Document Usage Estimate: a) Number of DMS users: b) Average number of documents per user: c) Average document size (bytes): d) Average number of versions per document: e) Total: (multiply a times b times c times d)	Calculate how much disk space the new library will need in order to help you select a location where you will store documents. For more information, see "Deciding Where to Store Documents" on page 279.
5) Document Storage Area Description:	Provide a brief description for the document storage area, including such information as which library it belongs to, its current capacity in megabytes, and the types of documents stored in it. For more information, see "Deciding Where to Store Documents" on page 279.
6) Document Storage Area Path:	Specify the UNC path to the location where you want to create the initial document storage area for the post office. For more information, see "Deciding Where to Store Documents" on page 279.
7) Library Description:	Provide a brief description for the new library, including what post office it belongs to, what types of documents will be stored in it, and so on. For more information, see "Deciding Which Libraries to Create" on page 274.
8) Start Version Number: ◆ 0 ◆ 1	Select 0 or 1. For more information, see "Setting Document Version Options" on page 281.

Item	Explanation
9) Maximum Archive Size:	Specify the maximum number of bytes to allow per archive directory. Use a size that conforms with your backup strategy and backup medium requirements. For more information, see "Figuring Maximum Archive Directory Size" on page 281.
10) Display Name:	Specify the library name you want users to see in the GroupWise client, if it is different from the Library object name. For more information, see "Choosing Library Names" on page 278.
11) Restrict Public Library Rights: ◆ Add ◆ Change ◆ Delete ◆ View ◆ Designate Official Version ◆ Reset In-Use Flag	Cross out any public library rights you do not want all users to have. For more information, see "Deciding Which Libraries to Create" on page 274 or "Setting Document Version Options" on page 281.
12) Librarians:	List any users you want to have full rights to all documents in the library. For more information, see "Designating Initial Librarians" on page 282.
13) Dedicated POA for Indexing ◆ Yes ◆ No	Mark whether or not you want to configure and run a separate POA dedicated to indexing documents. For more information, see "Determining Your Indexing Needs" on page 284.
14) Set Up Integrations ◆ Yes ◆ No	Mark whether or not you will need to manually set up integrations. For more information, see Chapter 24, "Integrations," on page 331.

23 Creating and Managing Documents

GroupWise® Document Management Services (DMS) lets Windows client users create documents with integrated applications, save them, then easily locate a specific document later without knowing the application, a specific document name, or the document's physical location. Windows client users can create, share, locate, edit, view, and check out documents that are created under the management of GroupWise DMS.

- "Adding Documents to Libraries" on page 303
- "Organizing Documents" on page 306
- "Indexing Documents" on page 319
- "Managing Documents" on page 328

NOTE: Cross-Platform client users have only basic DMS capabilities, as described in "Working with Documents" in *GroupWise 6.5 Cross-Platform Client User Guide*.

Adding Documents to Libraries

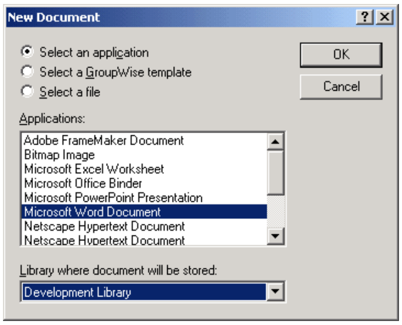
After you set up one or more libraries, users can add new documents to any library to which they have rights. They can also import existing documents into the GroupWise DMS system.

- "Creating New Documents in the GroupWise Windows Client" on page 303
- "Importing Existing Documents into the GroupWise DMS System" on page 304
- "Managing Groups of Documents" on page 305

Creating New Documents in the GroupWise Windows Client

To create a new document in the GroupWise Windows client:

1 Click File > New > Document.



New Document

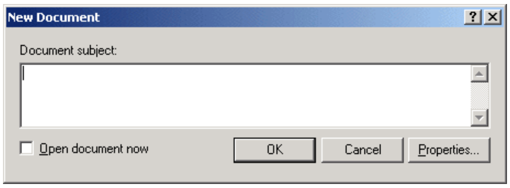
● Select an application
○ Select a GroupWise template
○ Select a file

Applications:
Adobe FrameMaker Document
Bitmap Image
Microsoft Excel Worksheet
Microsoft Office Binder
Microsoft PowerPoint Presentation
Microsoft Word Document
Netscape Hypertext Document
Netscape Hypertext Document

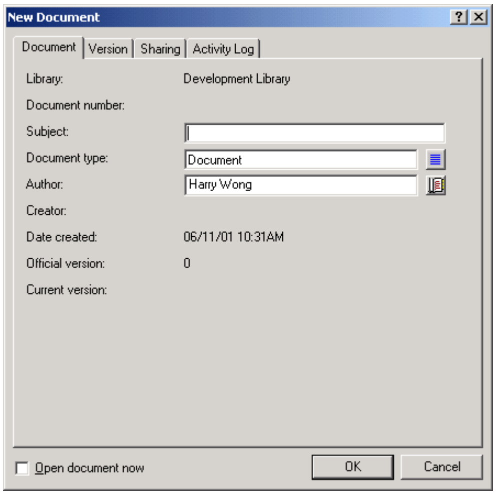
Library where document will be stored: Development Library

2 Select the program you want to use to create the document, select the library where you want to store the document, then click OK.

3 In the New Document dialog box, type a brief description of the document.



4 To set document properties, click Properties.



Library: Development Library

Document number:

Subject:

Document type: Document

Author: Harry Wong

Creator:

Date created: 06/11/01 10:31AM

Official version: 0

Current version:

5 Set the document properties as needed, then click OK.

The selected program starts so you can create a new document.

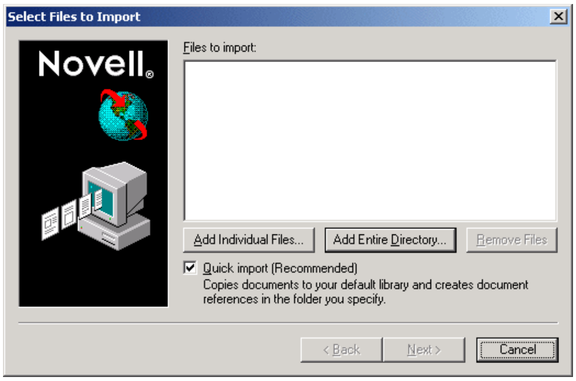
For more detailed information about creating documents in the GroupWise client, see "Creating Documents" in "Creating and Working with Documents" in the *GroupWise 6.5 Windows Client User Guide*. You can also look up "documents" in the GroupWise client help.

Importing Existing Documents into the GroupWise DMS System

Some users might have existing documents that they want to manage by adding them to a GroupWise library.

To import documents using the GroupWise Windows client:

1 Click File > Import Documents.



☑ Quick import (Recommended)
Copies documents to your default library and creates document references in the folder you specify.

2 Click Add Individual Documents, browse to and select the documents to add, then click OK.

or

Click Add Entire Directory, browse to and select a directory containing documents to import, then click OK.

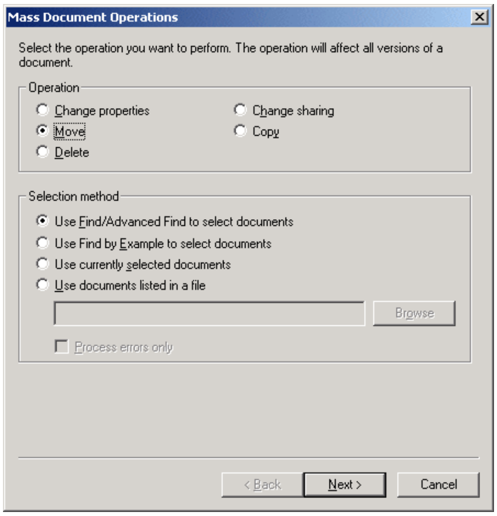
For additional instructions about creating documents in the GroupWise client, see "Importing Documents into a GroupWise Library" in "Creating and Working with Documents" in the *GroupWise 6.5 Windows Client User Guide*. You can also look up "import documents" in the GroupWise client help.

Managing Groups of Documents

As users add documents and your GroupWise DMS system grows, your librarians might need to assist users in managing large groups of documents. If you have not yet assigned librarians to your GroupWise libraries, see "Adding and Training Librarians" on page 295.

To manage large groups of documents in the GroupWise Windows client:

1 Click Tools > Mass Document Operations.



Select the operation you want to perform. The operation will affect all versions of a document.

Operation
○ Change properties
● Move
○ Delete
○ Change sharing
○ Copy

Selection method
● Use Find/Advanced Find to select documents
○ Use Find by Example to select documents
○ Use currently selected documents
○ Use documents listed in a file
□ Process errors only

2 Select the operation to perform on the group of documents:

- Change properties
- Move

- Delete
- Change sharing
- Copy

3 Select the method for identifying the group of documents to perform the operation on:

- Use Find/Advanced Find to select documents
- Use Find by Example to select documents
- Use currently selected documents
- Use documents listed in a file.

For additional instructions about creating documents in the GroupWise client, see "Managing Groups of Documents" in "Creating and Working with Documents" in the *GroupWise 6.5 Windows Client User Guide*. You can also look up "mass document operations" in the GroupWise client help.

Organizing Documents

Because documents are stored in a database structure, information can be associated with each document that is not part of the document itself. This additional information is stored as document properties.

- "Customizing Document Properties" on page 306
- "Defining Related Document Properties" on page 314

NOTE: Document properties cannot be set in ConsoleOne on Linux. However, you can use ConsoleOne on Windows to set document properties for libraries that are located on Linux.

Customizing Document Properties

For a summary of document properties, see "Document Properties" on page 265. To review, the following document properties are provided by default:

Author
Creator
Current Version Number
Date Created
Document Number
Document Type
Official Version Number
Subject

The default document property types cannot be deleted. Except for the Document Type property, they cannot be modified. However, you can add custom document types as needed.

- "Customizing the Default Document Type Property" on page 307
- "Planning Custom Document Properties" on page 308
- "Adding Custom Document Properties" on page 310
- "Planning Custom Lookup Tables for Custom Document Properties" on page 312
- "Adding Custom Lookup Tables" on page 313

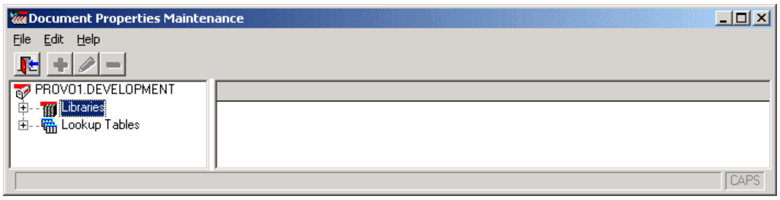
Customizing the Default Document Type Property

The Document Type property is the only default document property that you can modify. For a review of document types, see "Document Types" on page 266. You must have at least one document type, because it is a required document property field.

To modify the Document Type property for all libraries in a post office:

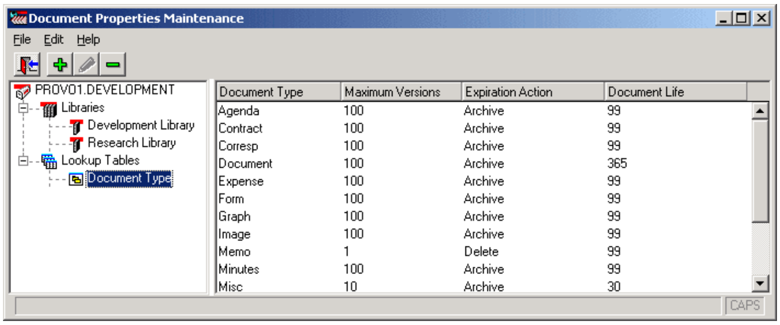
1 In ConsoleOne® on Windows, browse to and select the post office that has libraries where you want to modify the Document Type property.

2 Click Tools > GroupWise Utilities > Document Properties Maintenance.



If you expand Libraries and select each library, you will see that each library has the Document Type property. It is required.

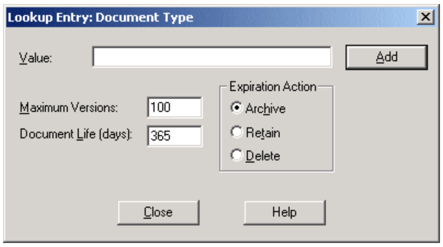
3 Expand Lookup Tables, then select Document Type.



Document Type	Maximum Versions	Expiration Action	Document Life
Agenda	100	Archive	99
Contract	100	Archive	99
Corresp	100	Archive	99
Document	100	Archive	365
Expense	100	Archive	99
Form	100	Archive	99
Graph	100	Archive	99
Image	100	Archive	99
Memo	1	Delete	99
Minutes	100	Archive	99
Misc	10	Archive	30

The lookup table defines the list of choices offered to users when they select a document type, no matter which library in the post office they are creating the document in.

4 To add a new document type, click Edit > Add. In the Value field, type the new document type, click Add, then click Close.



Value:

Maximum Versions: 100

Document Life (days): 365

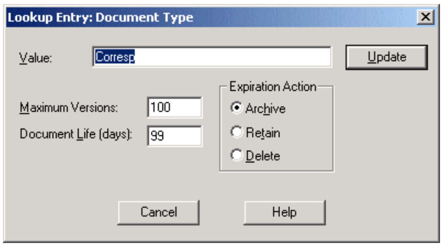
Expiration Action

● Archive

○ Retain

○ Delete

5 To edit an existing document type, click Edit > Edit. Change the settings as needed, click Update, then click Close.



Lookup Entry: Document Type

Value: Corresp

Maximum Versions: 100

Document Life (days): 99

Expiration Action

● Archive

○ Retain

○ Delete

For more details about the fields associated with the Document Type property, see "Document Types" on page 266.

6 To delete a document type, select the document type, click Edit, then click Delete.

Planning Custom Document Properties

When you need to add custom document properties, print the "Custom Document Properties Worksheet" on page 309. One copy of the worksheet accommodates three new document properties.

The following table describes the fields and values associated with custom document properties:

Document Property Field	Field Values
Property Field:	The document property field is the label that GroupWise client users will see in the document Properties dialog box. When you create a new document property, you can provide a description as well. However, the description displays only in ConsoleOne, not in the GroupWise client.
Read-Only?	**Yes:** The document property field will display information, but it will not be accessible to users. **No:** Users can type in the document property field.
Required?	**Yes:** The user must supply a value for the document property. **No:** The user can leave the document property field blank.
Hidden?	**Yes:** The document property field is not displayed in the GroupWise client interface. **No:** The document property field is displayed in the GroupWise client interface.
Lookup Table:	A lookup table is required for a custom document property only when you want to offer the user a list of choices, rather than having the user type in the setting. The lookup table guarantees that the user provides a valid setting. For more information, see "Planning Custom Lookup Tables for Custom Document Properties" on page 312.
Related Property:	A related property is required for a custom document property only when you create a lookup table that references a related lookup table. For more information, see "Defining Related Document Properties" on page 314.

Document Property Field	Field Values
Data Type:	**Binary:** An Object API reads and writes this information **Date:** Displayed in the Windows format selected by the user **Number:** Numerical only **String:** Alphanumeric
Maximum Length:	For the String data type, you can specify the maximum number of characters allowed in the string. The longest possible string is 65535 alphanumeric characters.
Case:	For the String data type, you can control how the user's input is handled: **Upper:** Forces entries to display in uppercase **Lower:** Forces entries to display in lowercase **Mixed:** Allows alphabetical characters to be displayed as typed
Minimum Value:	For the Number data type, you can specify a minimum acceptable value.
Maximum Value:	For the Number data type, you can specify a maximum acceptable value.
Parent:	If the new document property is related to an existing document property in a parent-child relationship, you must specify the parent document property. For more information, see "Defining Related Document Properties" on page 314.

Use copies of the "Custom Document Properties Worksheet" on page 309 to plan the custom document properties you want to add to libraries.

If you need to create one or more lookup tables for your custom document properties, follow the instructions in "Planning Custom Lookup Tables for Custom Document Properties" on page 312 and "Adding Custom Lookup Tables" on page 313. Lookup tables used by new document properties should exist before you create custom document properties.

Then continue with "Adding Custom Document Properties" on page 310.

Custom Document Properties Worksheet

For instructions on how to use this worksheet, see "Planning Custom Document Properties" on page 308.

Item	Custom Document Property	Custom Document Property	Custom Document Property
1) Post Office:			
2) Libraries:			
3) Property Label:			

Item	Custom Document Property	Custom Document Property	Custom Document Property
4) Description:			
5) Read-Only? ◆ Yes ◆ No			
6) Required? ◆ Yes ◆ No			
7) Hidden? ◆ Yes ◆ No			
8) Lookup Table:			
9) Data Type: ◆ Binary ◆ Date ◆ Number ◆ String			
10) Maximum Length:			
11) Case: ◆ Mixed ◆ Upper ◆ Lower			
12) Minimum Value:			
13) Maximum Value:			
14) Parent:			

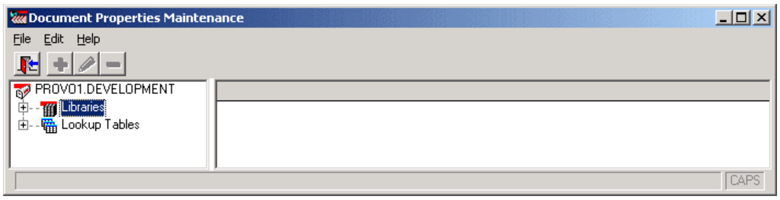
Adding Custom Document Properties

After you have determined what new document properties will meet the needs of your DMS system, as described in "Planning Custom Document Properties" on page 308, and if necessary you have created lookup tables for your new document properties, as described in "Planning Custom Lookup Tables for Custom Document Properties" on page 312 and "Adding Custom Lookup Tables" on page 313, you are ready to add new custom document properties.

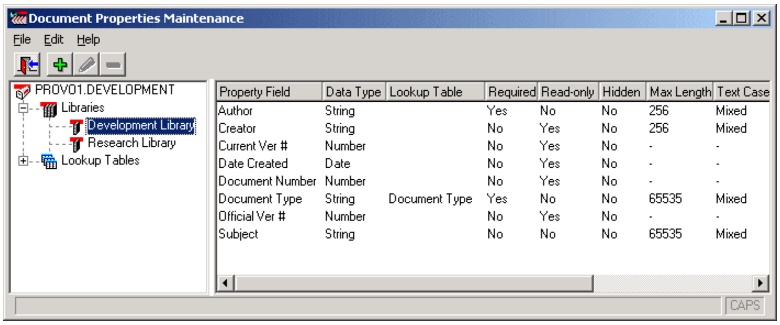
To add new custom document properties:

1 In ConsoleOne on Windows, browse to and select the Post Office object that owns the library for which you are creating custom document properties (worksheet item 1).

2 Click Tools > GroupWise Utilities > Document Properties Maintenance.

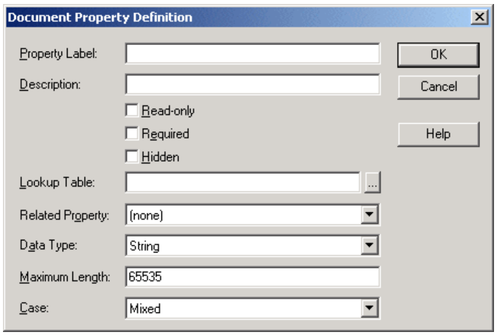


3 Expand Libraries, then select the library for which you are creating custom document properties (worksheet item 2).



Property Field	Data Type	Lookup Table	Required	Read-only	Hidden	Max Length	Text Case
Author	String		Yes	No	No	256	Mixed
Creator	String		No	Yes	No	256	Mixed
Current Ver #	Number		No	Yes	No	-	-
Date Created	Date		No	Yes	No	-	-
Document Number	Number		No	Yes	No	-	-
Document Type	String	Document Type	Yes	No	No	65535	Mixed
Official Ver #	Number		No	Yes	No	-	-
Subject	String		No	No	No	65535	Mixed

4 Click Edit > Add to display the Document Property Definition dialog box.



Property Label:

Description:

□ Read-only

□ Required

□ Hidden

Lookup Table:

Related Property: (none)

Data Type: String

Maximum Length: 65535

Case: Mixed

Fields vary according to data type.

5 Fill in the fields (worksheet items 3 through 14).

6 Click OK to create the new custom document property.

In the Document Properties Maintenance window, the new document property is listed in alphabetical order. In the GroupWise client, custom document properties are listed after default document properties, in the order in which they are added to the library.

7 Repeat Step 4 through Step 6 for each new custom document property.

When users next create documents in the library, the new custom document properties will be available to them.

Planning Custom Lookup Tables for Custom Document Properties

A lookup table is required for a custom document property only when you want to offer the user a list of choices, rather than having the user type in the setting. The lookup table guarantees that the user provides a valid setting.

Lookup tables are defined for the post office, so that multiple libraries in the post office can reference the same lookup tables.

When you need to provide lookup tables for custom document properties, print the "Custom Lookup Tables Worksheet" on page 313. One copy of the worksheet accommodates three new lookup tables.

The following table describes the fields and values associated with lookup tables:

Look Up Table Field	Field Values
Lookup Table Name:	The lookup table name identifies the lookup table when you are assigning it to a property field. If the lookup table pertains to only one document property, you can name the lookup table the same as the document property. For example, the default property Document Type uses a lookup table named Document Type. However, lookup tables can be used by multiple document properties. For example, you could have a lookup table named Project used by document properties named Primary Project and Secondary Project. When you create a new lookup table, you can provide a description as well. If the lookup table name does not match a document property, you could indicate what document properties use the lookup table.
Related Table:	A related table is required for a lookup table only when you want to define related properties. For more information, see "Defining Related Document Properties" on page 314.
Data Type:	**Binary:** An Object API reads and writes this information **Date:** Displayed in the Windows format selected by the user **Number:** Numerical only **String:** Alphanumeric
Maximum Length:	For the String data type, you can specify the maximum number of characters allowed in the string. The longest possible string is 65535 alphanumeric characters.
Case:	For the String data type, you can control how the user's input is handled: **Upper:** Forces entries to display in uppercase **Lower:** Forces entries to display in lowercase **Mixed:** Allows alphabetical characters to be displayed as typed
Minimum Value:	For the Number data type, you can specify a minimum acceptable value.
Maximum Value:	For the Number data type, you can specify a maximum acceptable value.
Lookup Table Entries:	The lookup table entries are the settings that users will choose from when they set the custom document property.

Use copies of the “Custom Lookup Tables Worksheet” on page 313 to plan the lookup tables you need in order to provide values for new custom document properties. If you need to use related properties, follow the instructions in “Defining Related Document Properties” on page 314. Then continue with “Adding Custom Lookup Tables” on page 313.

Custom Lookup Tables Worksheet

For instructions on how to use this worksheet, see “Planning Custom Lookup Tables for Custom Document Properties” on page 312.

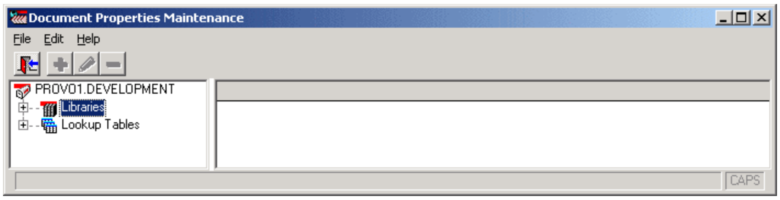
Item	Custom Lookup Table	Custom Lookup Table	Custom Lookup Table
1) Post Office:			
2) Property Label:			
3) Lookup Table Name:			
4) Description:			
5) Related Table:			
6) Data Type: ◆ Binary ◆ Date ◆ Number ◆ String			
7) Maximum Length:			
8) Case: ◆ Mixed ◆ Upper ◆ Lower			
9) Minimum Value:			
10) Maximum Value:			
11) Lookup Table Entries:			

Adding Custom Lookup Tables

After you have determined what new lookup tables and lookup table entries you need to accommodate your new custom document properties, as described in “Planning Custom Lookup Tables for Custom Document Properties” on page 312, you are ready to add new lookup tables.

1 In ConsoleOne on Windows, browse to and select the Post Office object that owns the libraries for which you are creating lookup tables (worksheet item 1).

2 Click Tools > GroupWise Utilities > Document Properties Maintenance.



3 Select Lookup Tables, then click Edit > Add to display the Lookup Table Definition dialog box.

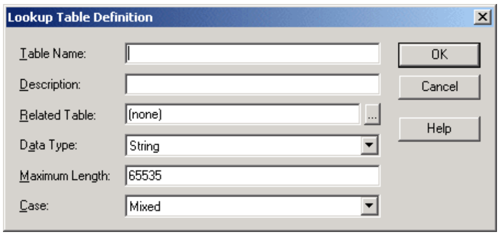


Table Name:

Description:

Related Table: (none)

Data Type: String

Maximum Length: 65535

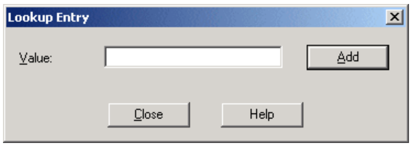
Case: Mixed

Fields vary depending on data type.

4 Fill in the fields (worksheet items 3 through 10).

5 Click OK to create the new lookup table.

6 Select the new lookup table, then click Edit > Add to display the Lookup Entry dialog box.



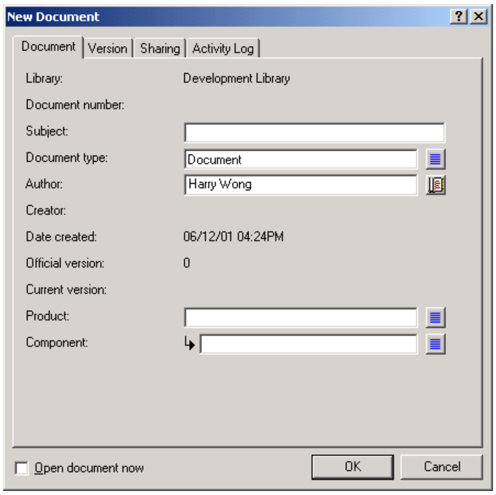
7 In the Value field, type one of the document property settings you want to offer to users (worksheet item 11), then click Add.

8 Repeat Step 7 for all the lookup table entries listed on your worksheet for this lookup table, then click Close.

9 Click OK to create the custom lookup table.

Defining Related Document Properties

When document properties are related, your choice for the first property determines the settings you are offered for the second property. For example, in the Development Library, custom document properties could be set up to indicate product and component information about every document in the library. Then, when users create new documents, Product and Component fields appear on the document Properties page.



Library: Development Library
Document number:
Subject:
Document type: Document
Author: Harry Wong
Creator:
Date created: 06/12/01 04:24PM
Official version: 0
Current version:
Product:
Component:

The user's selection in the Product field would determine what choices were offered in the Component field.

Related document properties are set up by creating related lookup tables. Complete the following tasks to set up related document properties:

- "Planning Related Document Properties" on page 315
- "Creating Related Lookup Tables" on page 317
- "Setting Up Related Document Properties" on page 318

Planning Related Document Properties

Related document properties use a parent-child relationship. A parent property can have multiple child properties, but a child property can belong to only one parent. The relationship can include only two levels. A parent property cannot function as a child and a child property cannot function as a parent. The default document properties cannot participate as related properties.

In the Development Library example above, the Product document property would be the parent property and the Component document property would be the child property. If the Development Library belonged to Novell®, products would include GroupWise, NetWare®, ZENworks®, and so on. When users selected GroupWise as the product, listed components could include the GroupWise client, the agents, GroupWise system administration, and so on. Or you could let users type in whatever components they wanted.

When you need to set up related document properties, print the "Related Document Properties Worksheet" on page 317. One copy of the worksheet accommodates one pair of related property fields, one parent lookup table, and one child lookup table (optional).

The following table describes the document properties and lookup tables that are required in order to set up related document properties:

Properties and Tables	Description
Parent Document Property	The parent document property is the user's first selection. In the Development Library example above, the parent document property is Product.

Properties and Tables	Description
Child Document Property	The child document property is the user's second selection, based on the first selection. In the Development Library example above, the child document property is Component.
Parent Lookup Table	The entries in the parent lookup table provide the choices offered to the user in the parent document property field. In the Development Library example above, the user could select from GroupWise, NetWare, and ZENworks in the Product field.
Child Lookup Table	The entries in the child lookup table provide the choices offered to the user after a choice from the parent lookup table has been selected. In the Development Library example above, if the user selected GroupWise in the Product field, the child lookup table would provide choices such as Agents, Client, and Admin in the Component field. The child lookup table is not required if you want to allow the user to type in anything they want in the child document property field.

Use copies of the "Related Document Properties Worksheet" on page 317 to plan the related document properties you want to use. One copy of the worksheet accommodates one pair of related properties. Continuing with the Development Library example, a filled-in worksheet might look like this:

Item	Setting	Item	Setting
1) Parent Document Property	Property Name: `Product`	4) Child Document Property	Property Name: `Component`
2) Parent Lookup Table	Table Name: `Product`	5) Child Lookup Table	Table Name: `Component`
3) Parent Lookup Entries	(required)	6) Child Lookup Entries	(optional)

	Parent Entry:
	`GroupWise`
			Child Entries:
			`Admin`
			`Agents`
			`Client`

	Parent Entry:
	`NetWare`
			Child Entries:
			`Client`
			`eDirectory`
			`Servers`

	Parent Entry:
	`ZENworks`
			Child Entries:
			`Desktops`
			`Servers`

When you have finished planning related properties and their associated lookup tables, you should print and fill in a worksheet for each for each new related property, as described in "Planning Custom Document Properties" on page 308, and for each new lookup table, as described in "Planning Custom Lookup Tables for Custom Document Properties" on page 312.

Then you are ready to continue with "Creating Related Lookup Tables" on page 317.

Related Document Properties Worksheet

For instructions on how to use this worksheet, see “Planning Related Document Properties” on page 315.

Item	Setting	Item	Setting
1) Parent Document Property	Name:	4) Child Document Property	Name:
2) Parent Lookup Table	Name:	5) Child Lookup Table	Name:
3) Parent Lookup Entries	(required)	6) Child Lookup Entries	(optional)
	Entry:		Entries:
	Entry:		Entries:
	Entry:		Entries:

Creating Related Lookup Tables

If you are supplying the choices for both related fields, you need both a parent lookup table and a child lookup table. If you are going to have users type information into the child property field, then you only need to create the parent lookup table. You should create lookup tables before creating the document properties that use them.

- “Creating the Parent Lookup Table” on page 317
- “Creating the Child Lookup Table (Optional)” on page 318

Creating the Parent Lookup Table

1. Create a new lookup table, as described in Step 1 through Step 5 in “Adding Custom Lookup Tables” on page 313. Use worksheet item 2 in the Table Name field. Leave the Related Table field set to (none).
2. Add entries to the new lookup table, as described in Step 6 through Step 8 in “Adding Custom Lookup Tables” on page 313. Use the entries listed under worksheet item 3 in the Value field.
3. Continue with “Creating the Child Lookup Table (Optional)” on page 318

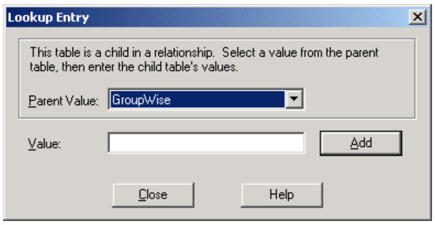
   or

If you are going to have users type information into the child property field, rather than selecting from a predefined list, skip to "Setting Up Related Document Properties" on page 318

Creating the Child Lookup Table (Optional)

1 Create a new lookup table, as described in Step 1 through Step 5 in "Adding Custom Lookup Tables" on page 313. Use worksheet item 5 in the Table Name field. Use worksheet item 2 in the Related Table field to link the child table to the parent table.

2 Select the new lookup table, click Edit, then click Add to display the Lookup Entry dialog box.



This table is a child in a relationship. Select a value from the parent table, then enter the child table's values.

Parent Value: GroupWise

Value:

3 Select a Parent value.

4 In the Value field, type one of the child lookup table entries for the selected parent value (worksheet item 6), then click Add.

5 Repeat Step 4 for each entry listed under worksheet item 6.

6 Repeat Step 3 through Step 5 for each parent value listed under worksheet item 3.

7 Continue with "Setting Up Related Document Properties" on page 318

Setting Up Related Document Properties

After you have created related lookup tables, you are ready to set up the related document properties that use them. A few document property fields are required settings in the context of related properties:

- Read-Only must be set to No.
- Hidden must be set to No.
- Required must be set the same on the child property as it is on the parent property.

To set up related document properties:

1 Create the parent document property as described in "Adding Custom Document Properties" on page 310. Use worksheet item 1 in the Property Label field. Use worksheet item 2 in the Lookup Table field. Leave the Related Property field set to (none).

2 Create the child document property using the same procedure. Use worksheet item 4 in the Property Label field. Use worksheet item 5 in the Lookup Table field. The Related Property field should automatically display as worksheet item 1, showing that the child property is related to the parent property.

Indexing Documents

Documents stored in GroupWise libraries need to be indexed so users can locate documents using the Find feature in the GroupWise Windows client. Your organization might need dedicated indexing to minimize performance degradation and network congestion. You might also need dedicated indexing so users can have prompt access to newly-created documents.

- "Understanding DMS Indexing" on page 319
- "Determining Your Indexing Needs" on page 326
- "Implementing Indexing" on page 327

Understanding DMS Indexing

Before determining if you will need dedicated indexing, you should have a basic understanding of how indexing works in GroupWise.

- "Index Storage" on page 319
- "Index Content" on page 319
- "Indexing Performed by the POA" on page 320
- "Indexing Cycle" on page 320
- "Bandwidth Considerations" on page 320
- "Indexer Configurations" on page 321

Index Storage

When documents are indexed, the information is stored in QuickFinder™ indexes, which are located in a library's index subdirectory. A library's QuickFinder index is partitioned into ten *.idx files. Additionally, temporary *.inc (incremental) files are created that contain each day's new index information. The *.inc files are combined once per day into the *.idx files (usually at midnight).

In a system with multiple libraries, each library has its own set of QuickFinder index files. Depending on how many libraries belong to a post office, and how many post offices with libraries are in your GroupWise system, there can be many sets of QuickFinder index files.

Index Content

Indexing can include a document's full text (depending on its document type), and always includes the document's property sheet information (subject, author, version descriptions, and so on). Both newly-edited and newly-created documents are indexed, which means indexing volume is determined by how many existing documents are edited as well as how many new documents are created.

Newly-created documents must be indexed before users can search for them. In setting up your indexing strategy, you must know how quickly users will need access to newly-created documents.

The standard search is limited to the QuickFinder indexes in the user's default library. But users can choose to search for documents in other libraries to which they have access.

Indexing Performed by the POA

Indexing is among the many functions of the Post Office Agent (POA). To learn more about POA functions, see "Role of the Post Office Agent" on page 423.

You can configure the POA for a post office to meet basic indexing needs. See "Regulating Indexing" on page 514.

To support greater indexing needs, you can set up an additional POA that is dedicated to indexing. See "Configuring a Dedicated Indexing POA" on page 516.

Not all libraries need dedicated POAs for indexing documents because indexing needs vary widely:

- In a small GroupWise system that has only one post office and one library, indexing can easily be done by the one POA.
- In a post office with heavy DMS usage, one or more additional POAs can be dedicated to indexing the documents.
- In a large system that has a DMS post office housing all libraries in the GroupWise system, indexing can be done by the DMS post office's POAs.

A library can have more than one POA dedicated to indexing its documents. Because the library's QuickFinder index is partitioned into ten separate *.idx files, an organization that is extremely document-intensive can boost indexing performance by using up to ten POAs dedicated to indexing. These POAs will not conflict with each other in performing indexing because the *.idx and *.inc files are locked during the indexing process.

You can temporarily use multiple indexing POAs for importing documents to speed up importing time.

Indexing Cycle

The frequency of indexing is determined by the POA QuickFinder Interval setting. The default is once every 24 hours at 8:00 p.m. This might be often enough in an organization where document usage is minimal, or where searching for newly-created documents is not mission-critical.

You can specify the QuickFinder Interval setting in one-hour increments. For example, a setting of 1 would allow users to find documents created as recently as an hour ago. Whether you should use a dedicated indexer at this frequency would depend on the volume (per hour) of documents that get queued for indexing.

You can set the QuickFinder Interval to 0 (zero) for continuous indexing. This is recommended for organizations where document usage is intensive, or where users routinely need to find documents that have just been created. If document usage is intensive in your organization, you might need a separate indexer server dedicated to continuous indexing because the post office server's performance could become unacceptably slow if continuous indexing is performed on it.

Bandwidth Considerations

A primary factor in network speed is bandwidth. This is the amount of data that can be passed through the network per second. If a network's bandwidth is not sufficient for handling heavy traffic, intensive document indexing can degrade network performance.

A number of elements affect network bandwidth: cable types, transmission protocols, and hardware. Ethernet networks are susceptible to wide fluctuations in transmission speed during periods of heavy traffic. WANs can benefit from reduced network traffic.

If you locate a post office in close proximity to its users, you will have less traffic through routers, bridges, and other network hardware. Running GroupWise in client/server access mode also reduces network traffic.

GroupWise users can add heavy messaging traffic to your existing network. DMS usage will add document indexing traffic as well. These factors could create much more network bandwidth usage than you have previously experienced.

Indexer Configurations

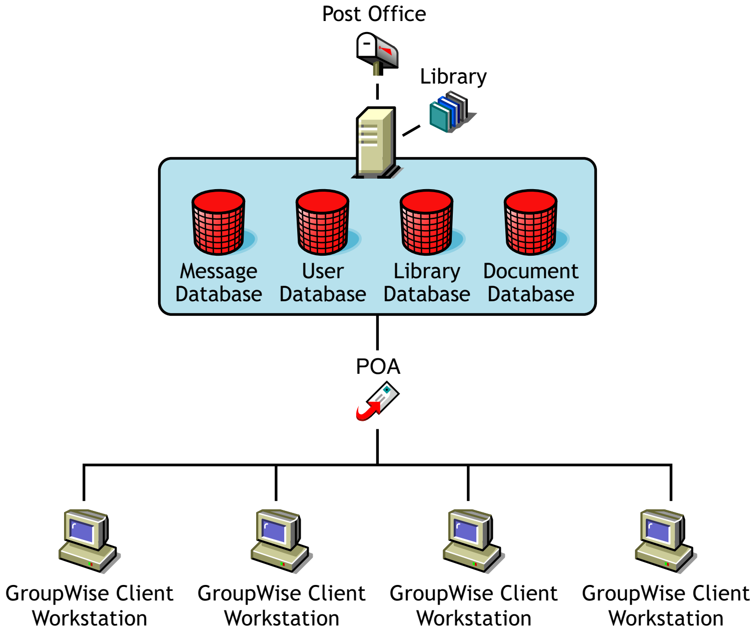
Following are five basic examples of how dedicated indexers can be configured. The examples do not cover all possibilities. You can combine elements from these configurations to customize indexing for your organization.

In all configuration examples, the post office can contain multiple libraries, although the Single Server with One POA configuration is best suited to only one library. In the other configuration examples, one or more POAs can be set up for indexing documents for all libraries in the post office.

- "Single Server with One POA" on page 321
- "Single Server with Multiple POAs" on page 322
- "Dedicated Indexer Server" on page 322
- "Dedicated Indexer Server on an Isolated Network Segment" on page 324
- "Dedicated DMS Post Office" on page 325

Single Server with One POA

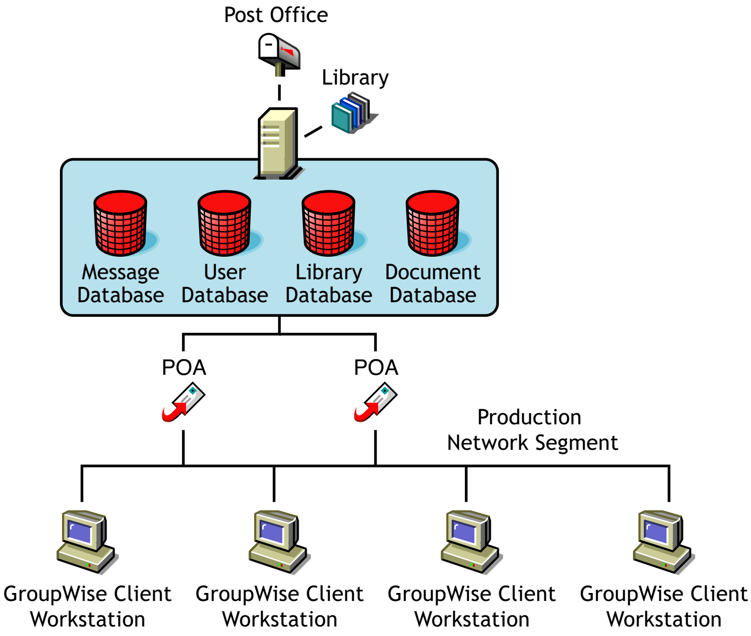
One POA runs on the post office server and performs all POA functions for the post office and its libraries. This basic configuration is best suited for a small system, or a decentralized library configuration with small post offices that each have a library. For more information, see "Centralized vs. Decentralized Library Configurations" on page 274.


Post Office
Library
Message Database
User Database
Library Database
Document Database
POA
GroupWise Client Workstation
GroupWise Client Workstation
GroupWise Client Workstation
GroupWise Client Workstation

Advantages	Disadvantages
- Default configuration; no additional setup is required. - Troubleshooting is limited to a single server.	- All operations are performed on one server, which can cause performance degradation if your organization does enough DMS operations. - If you increase QuickFinder intervals to lessen the load on the POA, you lengthen the time users must wait to search for new files, or find modified information through new searching keywords.

Single Server with Multiple POAs

It is possible to run more than one POA for the same post office on the same server.

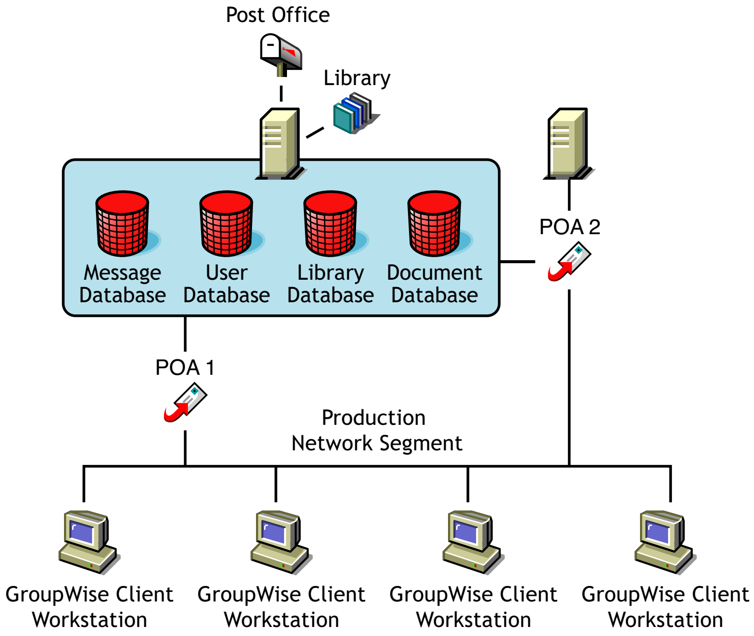

Post Office
Library
Message Database
User Database
Library Database
Document Database
POA
POA
Production Network Segment
GroupWise Client Workstation
GroupWise Client Workstation
GroupWise Client Workstation
GroupWise Client Workstation

Advantages	Disadvantages
None.	- Many processes running on one server can slow it down. - Single point of failure can cause the server to shut down when a problem is encountered.

There are no advantages to running multiple POAs on the same server. If you need more than one POA, run it on a separate server, as described in "Dedicated Indexer Server" on page 322

Dedicated Indexer Server

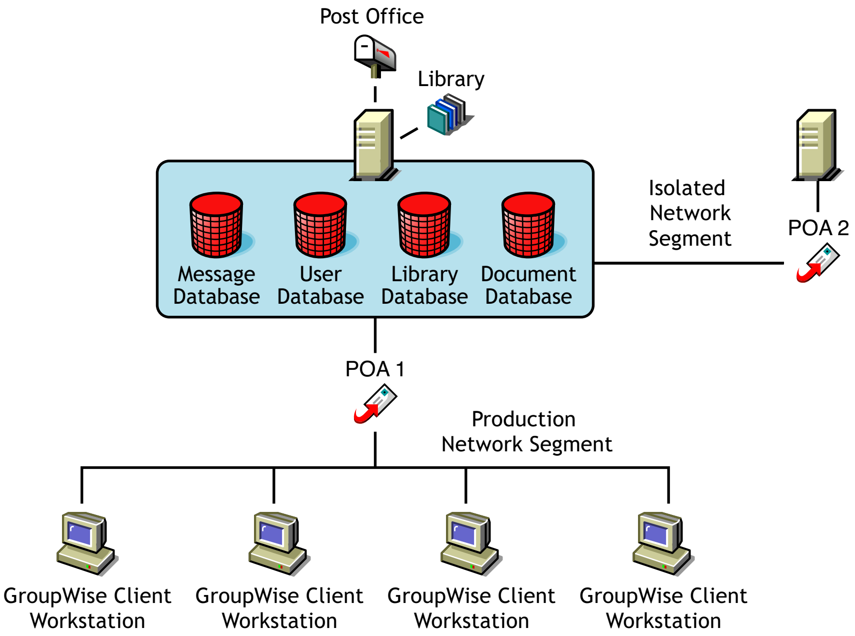
You can have the post office on one server and a POA dedicated to indexing DMS documents on another server. This configuration is useful for systems of any size with heavy DMS usage.


Post Office
Library
Message Database
User Database
Library Database
Document Database
POA 2
POA 1
Production Network Segment
GroupWise Client Workstation
GroupWise Client Workstation
GroupWise Client Workstation
GroupWise Client Workstation

Advantages	Disadvantages
◆ Dedicated server for quicker DMS indexing. This is useful for organizations that are document-intensive. ◆ Messaging post office is not hampered by DMS indexing.	◆ Network traffic can increase significantly during periods of intense indexing. ◆ Multiple server hardware is required.

Dedicated Indexer Server on an Isolated Network Segment

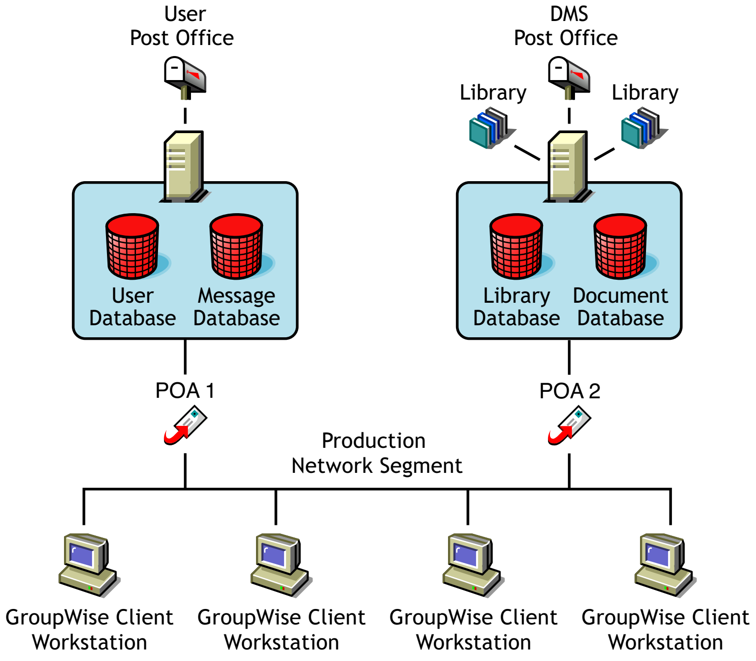
You can have the post office on one server and a POA dedicated to indexing documents on another server that is on an isolated network segment. This configuration minimizes bandwidth congestion for the production network segment.


Post Office
Library
Isolated Network Segment
POA 2
Message Database
User Database
Library Database
Document Database
POA 1
Production Network Segment
GroupWise Client Workstation
GroupWise Client Workstation
GroupWise Client Workstation
GroupWise Client Workstation

Advantages	Disadvantages
◆ Dedicated server for quicker DMS indexing. This is useful for organizations that are document-intensive. ◆ Messaging post office is not hampered by DMS indexing. ◆ The large amount of information that is passed between the post office server and the indexing server does not congest the bandwidth of the production network segment.	◆ Multiple server hardware is required. ◆ Dedicated network segment is required (including second network interface card that is directly linked to the indexer server). ◆ For multiple indexing servers, a dedicated hub might be needed.

Dedicated DMS Post Office

You can have one post office that is dedicated to messaging and another to DMS. This configuration is useful for post offices that have heavy DMS usage. For a review of this configuration, see "Centralized Libraries" on page 274.



Advantages	Disadvantages
◆ Dedicated POA for quicker DMS indexing. This is useful for organizations that are document-intensive. ◆ Messaging post office is not hampered by DMS traffic and indexing. ◆ Logical separation of messaging and DMS databases. Processes such as backing up databases are easier. ◆ This configuration is ideal for creating a centralized library configuration.	◆ High-end hardware is required for DMS server. ◆ Additional post office and POA to be maintained. ◆ Client/server is required for searching and accessing documents. ◆ Remote access is required for users who cannot use client/server mode. This ensures that the slower store-and-forward process will be used for remote searching and accessing of documents.

Determining Your Indexing Needs

The following table presents some indexing considerations and suggests an indexing configuration based on how the considerations pertain to your indexing needs:

Consideration	Single Server with One POA	Dedicated Indexer Server	Dedicated Indexer Server on an Isolated Network Segment	Dedicated DMS Post Office
Does the post office own multiple libraries?	No	Yes or No	Yes or No	Yes
What is the expected indexing volume (per hour)?	Light	Light or Moderate	Moderate or Heavy	Heavy
Is hardware available for a dedicated indexer server?	No	Yes	Yes	Yes
Could bandwidth congestion be a problem?	No	Maybe	Maybe or Yes	Yes

Use the "Indexing Worksheet" on page 327 to estimate the indexing needs of the libraries in your GroupWise system. Each worksheet accommodates three libraries.

Identify each library (worksheet items 1 and 2). Estimate the impact of each consideration in each library (worksheet items 3 through 6). Then compare your estimates for each library to the values in the table above to determine the indexing configuration for each library (worksheet item 7).

Indexing Worksheet

For instructions on how to use this worksheet, see “Determining Your Indexing Needs” on page 326.

	Library	Library	Library
1) Library:			
2) Library’s Post Office:			
3) Multiple Libraries per Post Office?			
◆ Yes			
◆ No			
4) Expected Indexing Volume (per hour):			
◆ Light			
◆ Moderate			
◆ Heavy			
5) Additional Server Available?			
◆ Yes			
◆ No			
6) Bandwidth Congestion Possible?			
◆ Yes			
◆ Maybe			
◆ No			
7) Indexer Configuration:			
◆ Single server with one POA			
◆ Dedicated indexer server			
◆ Dedicated indexer server on an insolated network segment			
◆ Dedicated DMS post office			

Implementing Indexing

For libraries where a single POA running on the post office server will provide adequate indexing support for the post office’s libraries, follow the instructions in “Regulating Indexing” on page 514 to implement indexing.

For libraries where additional POAs running on separate servers are required to support the indexing needs of the post office’s libraries, follow the instructions in “Configuring a Dedicated Indexing POA” on page 516 to implement indexing.

Managing Documents

As more and more documents are added to your GroupWise libraries, you will need to manage the disk space occupied by libraries and respond to various changes in your GroupWise system.

- "Archiving and Deleting Documents" on page 328
- "Backing Up and Restoring Archived Documents" on page 328
- "Handling Orphaned Documents" on page 329

See also "Managing Document Storage Areas" on page 290.

Archiving and Deleting Documents

The Document Type property determines what happens to documents whose document life in your GroupWise system has expired. For a review of the document types and document life, see "Document Types" on page 266.

You can use the Mailbox/Library Maintenance feature in ConsoleOne to archive and delete documents on demand, as described in "Reducing the Size of Libraries and Document Storage Areas" on page 371.

You can also configure the POA to archive and delete documents on a regular schedule, as described in "Scheduling Disk Space Management" on page 469.

Backing Up and Restoring Archived Documents

When documents are archived, they are physically moved to a directory in the post office, where disk space can be limited. You should move archived documents to your backup medium regularly.

- "Moving Archived Documents to Backup" on page 328
- "Restoring Archived Documents" on page 329

Moving Archived Documents to Backup

When documents are archived, they are placed in automatically created archive directories. Each library has a set of archive directories. For example, gwdms (GroupWise Document Management Services) is one of the post office's directories. The library directories exist under it, named lib00*01-ff*. Under each library directory is an archive directory, under which are the sequentially-numbered archival directories, named ar*nnnnnn* (where *nnnnnn* is an integer with leading zeros). Each ar*nnnnnn* directory is an archive set. To view the gwdms directory, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

To move archived documents to backup:

1. Make sure you have a backup medium (such as tape or CD) operating with your system.
2. Make sure you have already archived documents that have reached their expiration dates. Documents that have not been archived cannot be removed to a backup medium.
3. Start the software for your backup medium.
4. When the backup software asks for the location of your archive files, give the full path.

   Example: j:\post_office\gwdms\lib0\archive\ar000001

If users need the backed-up documents in the future, see "Restoring Archived Documents" on page 329.

Restoring Archived Documents

When a user tries to access a document that has been archived, one of two things will happen:

- If the document is in the post office archive set, and has not yet been physically moved from the archive location, the document opens normally. The user will not realize it was archived. The document is unarchived from the archive set at that time; that is, it is moved back to the library document directory from which it was archived. It is also given a new archive date according to the document type.
- The user will see a message indicating the document cannot be opened. In this case, the archive set containing the document has been physically moved to a backup medium. Therefore, the document cannot be automatically unarchived. In this case, the user might contact you, asking you to locate or recover the document. You can restore either the document's BLOB or the archive set that contains the BLOB. After the document is restored to its archive directory, the user will be able to open the document normally.

To restore archived documents from a backup medium:

1. Obtain the Document Number for the document the user was trying to access.
2. In the GroupWise Windows client, click Tools > Find.
3. Enter the Document Number, then click OK.
4. Right-click the document in the Find Results listing, then click Properties > Version.
5. Note the archive directory in the path listed in the Current Location field.

   The subdirectory listed after the ..\archive directory is the archive set containing the document, for example, \ar000001.
6. If you have the ability to recover individual files from your backup medium, also note the BLOB filename listed in the Current Filename field.
7. Determine where you backed up the archive set, then copy either the archive set or the individual BLOB file to the archive directory specified in the Current Location field that you noted earlier.
8. You can now notify the user that the requested document is available.
9. When you are sure the user has opened the document (causing it to be unarchived), you should delete any files remaining in that archive directory because you have already backed them up.

Handling Orphaned Documents

If you remove public rights for a library, some documents might become inaccessible. For example, if a user who has been denied access to the library is the only user that had access to certain documents, those documents become orphaned. No other user can access or search for those orphaned documents. This is because document security is controlled by the user listed in the Author and Creator fields in the document's properties. In other words, if the author or creator no longer has access to a document, neither will anyone else.

However, orphaned documents can be reassigned to another author so that someone can access them again. This can be done in one of two ways:

- In ConsoleOne, the Analyze/Fix Library action in Mailbox/Library Maintenance can reassign orphaned documents to a specified user. Then, the new user will have access to all orphaned documents in that library. For more information, see "Analyzing and Fixing Library and Document Information" on page 360.

- A librarian has the ability to alter the Author field of documents. Therefore, a librarian can replace the previous user’s GroupWise ID with his or her own ID. In doing so, the librarian becomes the new author of the document. This can also be done as a mass operation for multiple documents with varying user IDs in the Author field. For more information, see “Adding and Training Librarians” on page 295.

24 Integrations

Document-producing applications can be integrated with GroupWise® Document Management Services (DMS) to allow GroupWise management control over files produced by the integrated applications. Integrations provide code specifically designed to allow function calls, such as Open or Save, to be redirected to the GroupWise Windows client. This allows GroupWise dialog boxes to be displayed instead of the application's normal dialog boxes for the integrated functions.

NOTE: The Cross-Platform client does not include integrations, which is why you cannot create and edit documents from the Cross-Platform client.

GroupWise DMS includes standard integrations for the following applications:

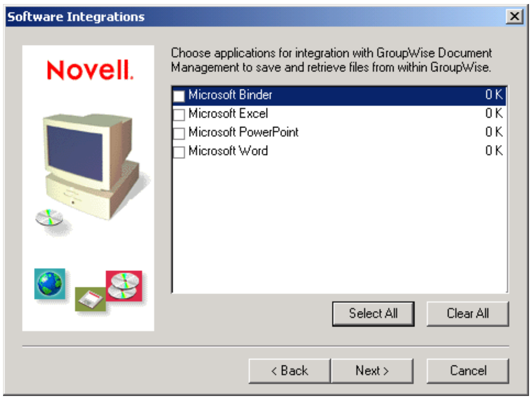
- Corel* Presentations* 7.*x* through 9.*x*
- Corel Quattro Pro* 7.*x* and 8.*x*
- Corel WordPerfect 6.1 through 9.*x*
- Lotus* Word Pro* 96 and 97
- Microsoft Binder 97
- Microsoft Excel 95 and 97
- Microsoft PowerPoint* 97
- Microsoft Word 95 and 97

Other applications can be integrated manually using the gwappint.inf file.

- "Setting Up Integrations during Windows Client Installation" on page 331
- "Setting Up Integrations Using the gwappint.inf File" on page 332
- "Controlling Integrations in the GroupWise Windows Client" on page 336

Setting Up Integrations during Windows Client Installation

The GroupWise Windows client installation program can offer users the opportunity to integrate their document-producing applications during client installation.



Choose applications for integration with GroupWise Document Management to save and retrieve files from within GroupWise.

□ Microsoft Binder	0 K
□ Microsoft Excel	0 K
□ Microsoft PowerPoint	0 K
□ Microsoft Word	0 K

This dialog box lists the applications that can be integrated with GroupWise that are currently installed on users' workstations. Therefore, it is important to make sure that the applications to integrate are installed *before* the GroupWise client is installed. However, it does not matter whether GroupWise and the applications are installed to run from the network or from the users' workstations. The integrations work with any combination of installation choices.

After selecting applications to integrate during GroupWise client integration, users can manage their integrations in the GroupWise client, as described in "Integrating GroupWise with Your Applications" in "Creating and Working with Documents" in the *GroupWise 6.5 Windows Client User Guide*.

If users need to install and integrate applications *after* installing the GroupWise client, they can install the new applications, then reinstall the GroupWise client so that they can select the new applications during GroupWise client installation. If reinstalling the GroupWise client is not an option, you might need to assist them in setting up additional integrations, as described in "Setting Up Integrations Using the gwappint.inf File" on page 332.

Setting Up Integrations Using the gwappint.inf File

The gwappint.inf file controls how document-producing applications are integrated with GroupWise. During GroupWise client installation, it is installed in the Windows system32 subdirectory. It is a text file that can be viewed and modified in a text editor such as Notepad. You might want to print the gwappint.inf file from a user workstation to help you understand how integrations have been set up for your users during GroupWise client installation.

- "Understanding the Three Levels of Integration" on page 332
- "Understanding the gwappint.inf File" on page 333
- "Editing the gwappint.inf File" on page 336

Understanding the Three Levels of Integration

The gwappint.inf file provides for three different levels of integration, to meet the needs of different types of document-producing applications:

- "ODMA Integration" on page 333
- "Point-to-Point Integration" on page 333
- "No Integration" on page 333

ODMA Integration

The Open Document Management API (ODMA) is an industry standard for applications and document management programs to use in achieving seamless integration. ODMA is platform-independent. GroupWise DMS is 32-bit ODMA-compliant, and can automatically integrate with all 32-bit ODMA-compliant applications. Applications that are not 32-bit ODMA-compliant must have integrations created for them to be used with GroupWise DMS.

The 16-bit ODMA integration standards are not 100% compatible with the 32-bit ODMA integration in Windows 95/98/2000. Therefore, 16-bit applications that are ODMA-compliant must still have integrations created for them to be used with the GroupWise DMS.

Point-to-Point Integration

This integration involves applications that are not 32-bit ODMA-compliant. Novell® has written macros for various applications, such as Microsoft Word, which allow them to be integrated with GroupWise. This provides the same functionality as for 32-bit ODMA-integrated applications. These applications can be selected for integration when the GroupWise client is installed.

Integration macros are written in the macro language of the application being integrated with GroupWise. Macro calls are made to GroupWise dialog boxes to replace access of the application's own dialog boxes (for example, Open and Save).

No Integration

Non-integrated applications rely on Windows 95/98/2000 associations. When a reference icon is selected in GroupWise, the file's extension is examined to determine which application to use. The application is launched and the file is opened.

Functions performed in a non-integrated application are not managed by GroupWise. So, if the file is renamed or saved to a different location, the file will not be part of a GroupWise library. When the file is opened later, a message will be displayed reminding the user that the file is not under management of GroupWise. However, if you simply edit the file and re-save it without changing the name or location, GroupWise will continue to provide management of the file.

Understanding the gwappint.inf File

The gwappint.inf file includes the following sections and lines:

- [*executable_name*] sections
  - Integration= line
  - DualExe= line
  - AppName= line
  - AppKey= line
- [ODMA Application Extensions] section
- [Integration State] section
- [Non-Integrated Defaults] section
  - WaitInterval= line
  - ShowMessage- line

[*executable_name*] Sections

The gwappint.inf file contains one [*executable_name*] section for each integrated application. It supplies the name of the executable for the program being integrated.

Integration= Line

Each [*executable_name*] section must have an Integration= line, where digits identify the type of integration employed for the executable:

Integration = 0 (No Integration)
Integration = 1 (Point-to-Point Integration)
Integration = 2 (ODMA Integration)

DualExe= Line

Some programs, such as Lotus Word Pro, use a small startup executable that, in turn, calls the main program. Use the DualExe= line to specify the name of the main executable. You can specify the full path to the main executable, or you can specify the path relative to the startup executable.

AppName= Line

The AppName= line assigns the application an arbitrary name for use in the [ODMA Application Extensions] and [Integration State] sections.

AppKey= Line

The AppKey= line is used only with point-to-point integrations (Integration=1). It specifies a value used by GroupWise to pass information to and from the integrated application. The value must be unique among the point-to-point integrations defined in the gwappint.inf file.

Examples Based on Standard Integrations

The table below shows how the standard integrations are implemented in the gwappint.inf file:

Application	Executable	Version	Comments
Corel Presentations	prwin.exe	3	If it is already installed on the workstation, GroupWise installation will change the Integrations= line to 0 and the application will be available for selection as a non-integrated application.
		7	For ODMA integration, change the DualExe= line to SYSTEM\PRWIN70.EXE and the Integrations= line to 2.
		8	For ODMA integration, change the Integrations= line to 2.
Corel Quattro Pro	qpw.exe	6.1	If it is already installed on the workstation, the GroupWise client installation will change the Integrations= line to 0 and the application will be available for selection as a non-integrated application.
		7	For ODMA integration, change the Integrations= line to 2
Corel WordPerfect	wpwin.exe	6.1	If it is already installed on the workstation, the GroupWise client installation will change the Integrations= line to 0 and the application will be available for selection as a non-integrated application.
		7	For ODMA integration, change the DualExe= line to SYSTEM\WPWIN7.EXE and the Integrations= line to 2.

Application	Executable	Version	Comments
Lotus Word Pro	wordpro.exe	96	This application is 32-bit ODMA-compliant. Therefore, if installed before GroupWise, it will be available for selection as an ODMA-integrated application.
		97	For ODMA integration, change the DualExe= line to SYSTEM\WORDPRO.EXE and the Integrations= line to 2.
Microsoft Binder	binder.exe	97	This application is 32-bit ODMA-compliant. Therefore, if installed before GroupWise, it will be available for selection as an ODMA-integrated application.
Microsoft Excel	excel.exe	95 and 97	The Integrations= line will be set to 1 for both versions.
Microsoft PowerPoint	powerpnt.exe	97	This application is 32-bit ODMA-compliant. Therefore, if installed before GroupWise, it will be available for selection as an ODMA-integrated application.
Microsoft Word	winword.exe	95	If it is already installed on the workstation, GroupWise installation will change the Integrations= line to 1 and the application will be available for selection for point-to-point integration.
		97	For ODMA integration, change the Integrations= line to 2.

[ODMA Application Extensions] Section

The [ODMA Application Extensions] section lists the file extensions GroupWise associates with particular document-producing applications. Examples include:

Application	File Extension
Corel WordPerfect	.wpd
Microsoft Excel	.xls
Microsoft PowerPoint	.ppt
Microsoft Word	.doc

[Integration State] Section

The [Integration State] section records whether the user has turned integrations on or off for integrated applications.

[Non-Integrated Defaults] Section

The [Non-Integrated Defaults] section provides two configuration settings that apply to all non-integrated applications:

- WaitInterval= line
- ShowMessage= line

WaitInterval= Line

The WaitInterval= line specifies a number of milliseconds for the GroupWise client to wait before it attempts to communicate with a non-integrated process. The wait interval allows the application to start completely before GroupWise contacts it. The default wait interval is 1000 milliseconds (one second).

The default setting supplied in the [Non-Integrated Defaults] section can be overridden for specific applications by including a WaitInterval= line in the application's [*executable_name*] section.

ShowMessage= Line

The ShowMessage= line indicates whether or not to display a message to the GroupWise client user if GroupWise cannot contact a non-integrated application. Use ShowMessage=1 to display the message or ShowMessage=0 to suppress the message.

The default setting supplied in the [Non-Integrated Defaults] section can be overridden for specific applications by including a ShowMessage= line in the application's [*executable_name*] section.

Editing the gwappint.inf File

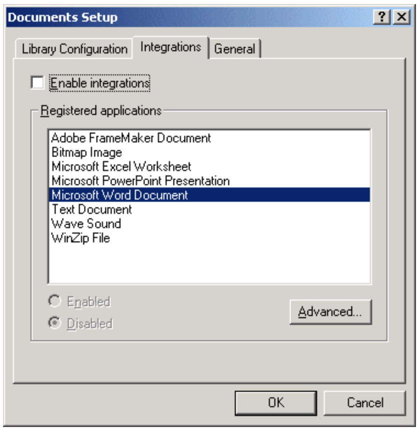
The gwappint.inf file is a text file that can be modified using any text editor (Notepad, for example). By editing the gwappint.inf file, you can add integrations for applications for which Novell has not provided integrations.

Controlling Integrations in the GroupWise Windows Client

For the convenience of GroupWise Windows client users, some settings in the gwappint.inf file can be modified from the client.

In the GroupWise client:

1 Click Tools > Options > Documents > Integrations.



□ Enable integrations

Registered applications

- Adobe FrameMaker Document
- Bitmap Image
- Microsoft Excel Worksheet
- Microsoft PowerPoint Presentation
- Microsoft Word Document
- Text Document
- Wave Sound
- WinZip File

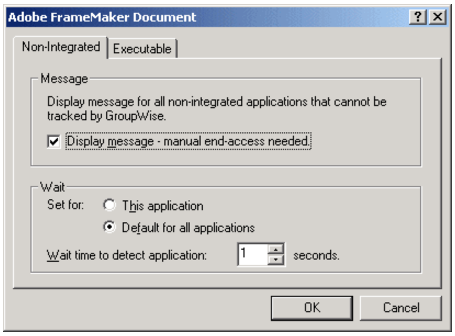
○ Enabled
● Disabled

The Integrations tab of the Documents Setup dialog box lets users turn integrations on and off for the listed registered applications.

If the application that users want to integrate is does not appear in the registered applications list, users must first make sure the application is installed on their workstations. They they can either reinstall the GroupWise client or modify the gwappint.inf file as described in "Setting Up Integrations Using the gwappint.inf File" on page 332.

The users' selections on the Integrations tab are recorded in the [Integration State] section of the gwappint.inf file.

2 Select an application to configure integration for, then click Advanced.



Adobe FrameMaker Document

Message

Display message for all non-integrated applications that cannot be tracked by GroupWise.

☑ Display message - manual end-access needed.

Wait

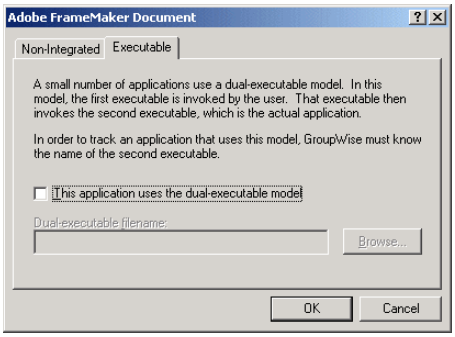
Set for: ○ This application

● Default for all applications

Wait time to detect application: 1 seconds.

The Non-Integrated tab enables users to set values for the ShowMessage= and WaitInterval= lines in the gwappint.inf file.

3 Click Executable.



Adobe FrameMaker Document

A small number of applications use a dual-executable model. In this model, the first executable is invoked by the user. That executable then invokes the second executable, which is the actual application.

In order to track an application that uses this model, GroupWise must know the name of the second executable.

□ This application uses the dual-executable model

Dual-executable filename:

The Executable tab enables users to set the DualExe= line in the gwappint.inf file.

4 Click OK twice to save the updated integration information.

If users check the contents of the gwappint.inf file in the Windows system32 subdirectory, they will see their integration configuration changes reflected there.

VIII Databases

25 Understanding GroupWise Databases

Your GroupWise® system includes numerous databases where vital information is stored.

Domain Databases

The domain database (wpdomain.db) in each domain contains all administrative information for the domain, including:

- Address information about all GroupWise objects (such as users and resources), post offices, and gateways in the domain
- System configuration and linking information for the domain's MTA
- Address and message routing information to other domains

The first domain you create is the primary domain. In the primary domain, the wpdomain.db file contains all administrative information for your entire GroupWise system (all domains, post offices, users, and so on). Because the wpdomain.db file in the primary domain is so crucial, you should back it up regularly and keep it secure. See "Backing Up a Domain" on page 375.

You can re-create your entire GroupWise system from the primary domain wpdomain.db file; however, if the primary domain wpdomain.db file becomes unusable, you can no longer make administrative updates to your GroupWise system.

In a secondary domain, the wpdomain.db file contains administrative information about that secondary domain only.

For the location of the domain database, see "Domain Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. For additional domain information, see "Information Stored in the Domain" on page 558.

Post Office Databases

The post office database (wphost.db) in each post office contains all administrative information for the post office, including a copy of the GroupWise Address Book. This information is necessary for users to send messages to others in the GroupWise system.

For the location of the post office database, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. For more post office information, see "Information Stored in the Post Office" on page 418.

User Databases

Each member of the post office has a personal database (user*xxx*.db) which represents the user's mailbox. The user database contains the following:

- Message header information
- Pointers to messages
- Personal groups
- Personal address books
- Rules

When a member of another post office shares a folder with one or more members of the local post office, a "prime user" database (pu*xxxxx*.db) is created to store the shared information. The "prime user" is the owner of the shared information.

Local user databases and prime user databases are stored in the ofuser directory in the post office.

Because resources are addressable just like users, resources also have user databases.

For the location of user databases in the post office, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. For more post office information, see "Information Stored in the Post Office" on page 418.

Message Databases

Each member of the post office is assigned to a message database (msg*nn*.db) where the body portions of messages are stored. Many users in a post office share a single message database. There can be as many as 25 message databases in the post office. Message databases are stored in the ofmsg directory in the post office.

Outgoing messages from local senders are stored in the message database assigned to each sender. Incoming messages from users in other post offices are stored in the message database with the same name as the message database assigned to the sender in his or her own post office. In each case, only one copy of the message is stored in the post office, no matter how many members of the post office it is addressed to.

For the location of message databases in the post office, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. For more post office information, see "Information Stored in the Post Office" on page 418.

Library Databases

A library is a collection of documents and document properties stored in a database system that can be managed and searched. You do not need to set up libraries unless you are using GroupWise Document Management Services (DMS). See "Libraries and Documents" on page 261.

The databases for managing libraries are stored in the gwdms directory and its subdirectories in the post office.

The dmsh.db file is a database shared by all libraries in the post office. It contains information about where each library in the post office is located.

Each library has its own subdirectory in the gwdms directory. In each library directory, the dm*xxnn01-FF*.db files contain information specific to that library, such as document properties and what users have rights to access the library.

For the location of library databases in the post office, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. For more post office information, see "Information Stored in the Post Office" on page 418.

The actual documents in a library are not kept in the library databases. They are kept in a document storage area, which consists of a series of directories for storing documents. Documents are encrypted and stored in BLOBs (binary large objects) to make document management easier. A document, its versions, and related objects are stored together in the same BLOB.

A document storage area might be located in the post office itself, or in some other location where more storage space is available. If it is located in the post office, the document storage area can never be moved. Therefore, storing documents in the post office directory structure is not usually recommended. If it is stored outside the post office, a document storage area can be moved when additional disk space is required.

See Chapter 22, "Creating and Managing Libraries," on page 269 and Chapter 23, "Creating and Managing Documents," on page 303 for more information about Document Management Services.

Guardian Databases

The guardian database (ngwguard.db) serves as a reference for the following subordinate databases in the post office:

- User databases (user*xxx*.db)
- Message databases (msg*nn*.db)
- Prime user databases (pu*xxxxx*.db)
- Library databases (dmsh.db and dm*xxnn01-FF*.db)

The guardian database stores information that is common among all databases, thus eliminating duplication of information. The subordinate databases reference information stored in the guardian database. The benefits of the guardian database include the following:

- **Single Reference Point:** The guardian database stores information for each post office. Instead of storing the dictionary information in multiple dictionary databases, it is stored once in the guardian database.
- **Increased Performance:** When the information in the guardian database is accessed, it is written to cache memory. Each subsequent request can be handled with information already available in cache memory, which is faster than disk access.
- **Tracking Attachments and Documents:** When an attachment or document becomes orphaned (loses pointers to the message or profile), the guardian database is used to re-locate the origination of the attachment or document.
- **GroupWise Remote Management:** When a user starts GroupWise Remote, a local guardian database is created on the remote workstation to store information similar to the guardian database in the remote user's post office in the master system.

The guardian database is vital to GroupWise functioning. Therefore, the POA has an automated back-up and roll-forward process to protect it. The POA keeps a known good copy of the guardian database called ngwguard.fbk. Whenever it modifies the ngwguard.db file, the POA also records the transaction in the roll-forward transaction log called ngwguard.rfl. If the POA detects damage to the ngwguard.db file on startup or during a write transaction, it goes back to the ngwguard.fbk file (the "fall back" copy) and applies the transactions recorded in the ngwguard.rfl file to create a new, valid and up-to-date ngwguard.db.

In addition to the POA back-up and roll-forward process, you should still back up the ngwguard.db, ngwguard.fbk, and ngwguard.rfl files regularly to protect against media failure. Without a valid ngwguard.db file, you cannot access your e-mail. With current ngwguard.fbk and ngwguard.rfl files, you can rebuild a valid ngwguard.db file should the need arise.

The ngwguard.dc file is the structural template for building the guardian database and its subordinate databases. Also called a dictionary file, the ngwguard.dc file contains schema extension information, such as administrator-defined fields, data types, and record indexes. If this dictionary file is missing, no additional databases can be created in the post office.

26 Maintaining Domain and Post Office Databases

Occasionally, it is necessary to perform maintenance tasks on domain databases (wpdomain.db) or post office databases (wphost.db). The frequency depends on the reliability of your network and your own experience of how often problems are likely to occur. The following tasks help you maintain the integrity of your domain and post office databases:

- "Validating Domain or Post Office Databases" on page 345
- "Recovering Domain or Post Office Databases" on page 346
- "Rebuilding Domain or Post Office Databases" on page 349
- "Rebuilding Database Indexes" on page 351

NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

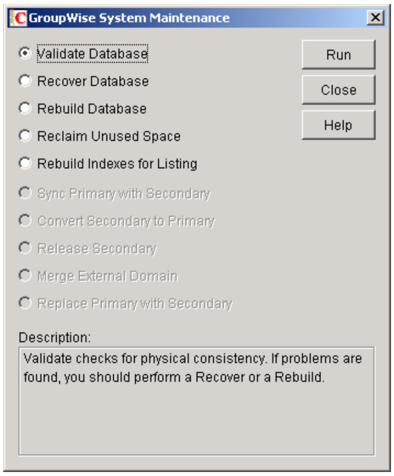
To further protect your GroupWise® system against loss of domain and post office information, see Chapter 31, "Backing Up GroupWise Databases," on page 375 and Chapter 32, "Restoring GroupWise Databases from Backup," on page 379.

To ensure that the same information exists in all domain and post office databases throughout your GroupWise system, see "Synchronizing the Primary Domain from a Secondary Domain" on page 366, "Synchronizing a Secondary Domain" on page 365, and "Synchronizing a Post Office" on page 364.

Validating Domain or Post Office Databases

You can validate the data in the domain and post office databases at any time without interrupting normal GroupWise operation. The frequency can vary depending on the size of your system and the number of changes you make to users, resources, and distribution lists.

1. Make sure you have full administrative rights to the domain and post office database directories you are validating.
2. In ConsoleOne®, browse to and select the Domain object or Post Office object where you want to validate the database.
3. Click Tools > GroupWise Utilities > System Maintenance.


GroupWise System Maintenance
● Validate Database
○ Recover Database
○ Rebuild Database
○ Reclaim Unused Space
○ Rebuild Indexes for Listing
○ Sync Primary with Secondary
○ Convert Secondary to Primary
○ Release Secondary
○ Merge External Domain
○ Replace Primary with Secondary
Run
Close
Help

Description:

Validate checks for physical consistency. If problems are found, you should perform a Recover or a Rebuild.

4. Click Validate Database > Run.
5. When prompted, make sure the Path to Database is correct. If an incorrect path is displayed, browse to and select the path to the database being validated. Click OK.

   You will be notified if there are any physical problems, so you can then recover or rebuild the database.

   See "Recovering Domain or Post Office Databases" on page 346 and "Rebuilding Domain or Post Office Databases" on page 349.

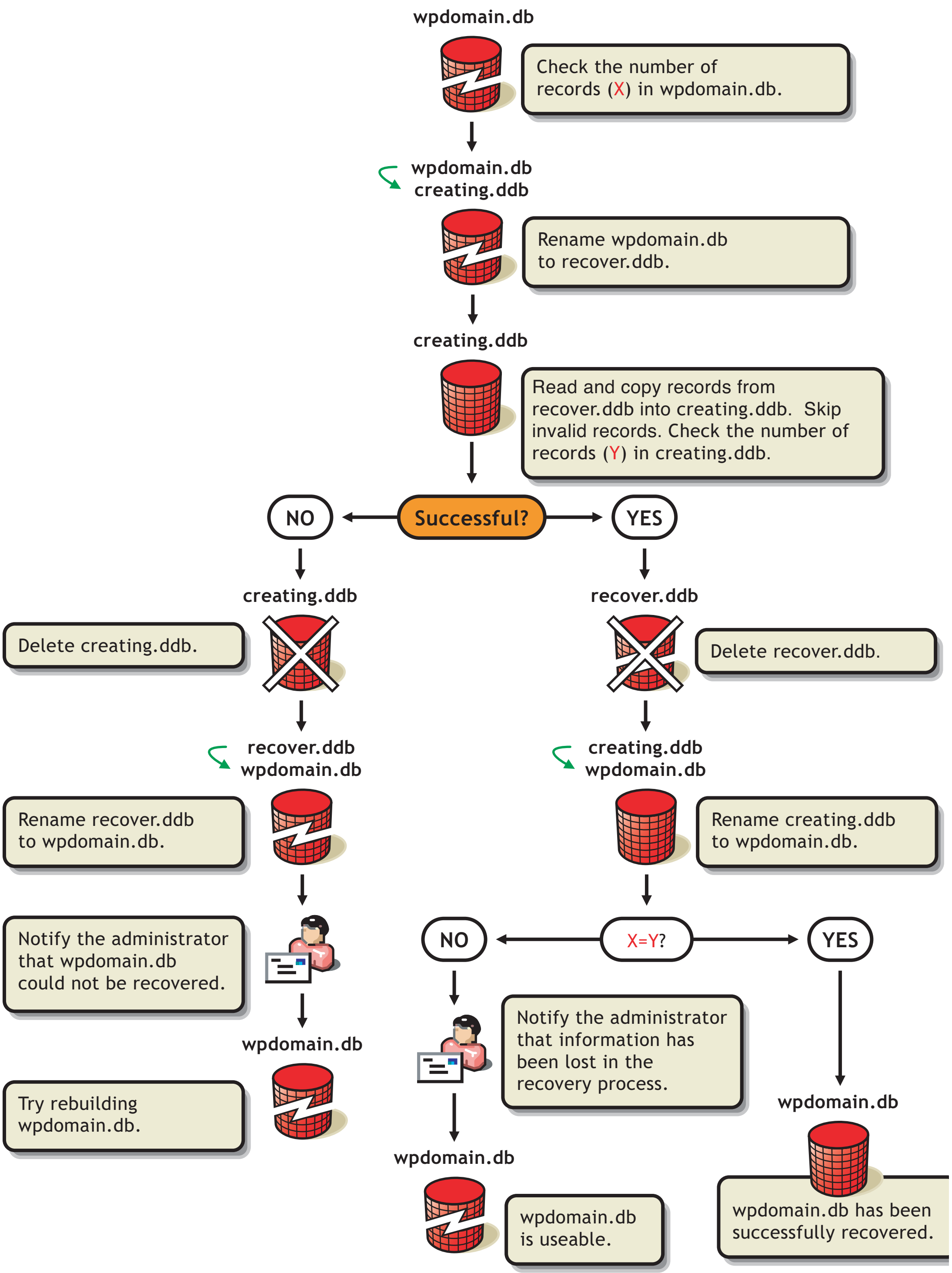
Recovering Domain or Post Office Databases

The database recover process corrects physical problems in the database structure, but does not update incorrect information contained in the database.

If you receive an administrative message informing you that an internal database error has occurred, or if you detect database damage and don't want to take users out of GroupWise, you can recover the database. If no errors are reported after the recover process, you will not need to take further action.

The recover process is run against a copy of the domain database (wpdomain.db) or post office database (wphost.db). Therefore, while the recover process is being run, you can continue to access the database through ConsoleOne and you do not need to stop the MTA or the POA.

As the copy of the database is created, the recover process skips invalid records. If the number of records in the original wpdomain.db file or wphost.db file is different from the number in the new, valid copy, GroupWise will send an administrative message informing you that data has been lost. When the recover process is completed, the backup database will be deleted.


wpdomain.db
Check the number of records (X) in wpdomain.db.
wpdomain.db
creating.ddb
Rename wpdomain.db to recover.ddb.
creating.ddb
Read and copy records from recover.ddb into creating.ddb. Skip invalid records. Check the number of records (Y) in creating.ddb.
NO
Successful?
YES
creating.ddb
Delete creating.ddb.
recover.ddb
Delete recover.ddb.
recover.ddb
wpdomain.db
Rename recover.ddb to wpdomain.db.
creating.ddb
wpdomain.db
Rename creating.ddb to wpdomain.db.
Notify the administrator that wpdomain.db could not be recovered.
NO
X=Y?
YES
Notify the administrator that information has been lost in the recovery process.
wpdomain.db
Try rebuilding wpdomain.db.
wpdomain.db
wpdomain.db
wpdomain.db is useable.
wpdomain.db has been successfully recovered.

For convenience, the agents are configured by default to automatically recover domain and post office databases whenever a physical problem is encountered. See "Recovering the Domain Database Automatically or Immediately" on page 614 and "Recovering the Post Office Database Automatically or Immediately" on page 485.

To recover a specific database in ConsoleOne:

1 Make sure you have network access to the domain or post office directory for the database you are recovering.

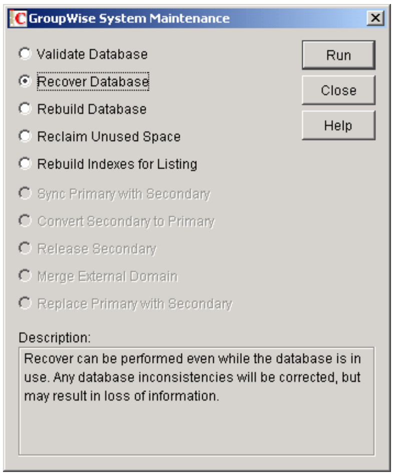
If you have administration rights in the primary domain, you can recover the primary domain database, the post office databases in the primary domain, and any secondary domain databases.

From a secondary domain, you can recover the secondary domain database and the post office databases in the secondary domain.

2 Make sure you have sufficient disk space for the copy of the database that is created during recovery.

3 In ConsoleOne, browse to and select the Domain object or Post Office object where you want to recover the database.

4 Click Tools > GroupWise Utilities > System Maintenance.



○ Validate Database
● Recover Database
○ Rebuild Database
○ Reclaim Unused Space
○ Rebuild Indexes for Listing
○ Sync Primary with Secondary
○ Convert Secondary to Primary
○ Release Secondary
○ Merge External Domain
○ Replace Primary with Secondary

Description:
Recover can be performed even while the database is in use. Any database inconsistencies will be corrected, but may result in loss of information.

5 Click Recover Database > Run.

6 When prompted, make sure the Path to Database is correct. If an incorrect path is displayed, browse to and select the path to the database being validated. Click OK.

If recovery is successful, the backup database is deleted, and the new domain database is renamed to wpdomain.db, or the new post office database is renamed to wphost.db.

If recovery fails for any reason, the backup database will be copied back to wpdomain.db or wphost.db. If any data was lost, you will be notified by an administrative message.

You have several options for retrieving lost data from other sources:

- If data has been lost from the primary domain, you can synchronize it with a secondary domain that is known to contain current information. See "Synchronizing the Primary Domain from a Secondary Domain" on page 366.
- If data has been lost from a secondary domain, you can synchronize it with the primary domain. See "Synchronizing a Secondary Domain" on page 365.
- You can also rebuild the database at a later time when you have exclusive access to the database where the data has been lost. See "Rebuilding Domain or Post Office Databases" on page 349.

Rebuilding Domain or Post Office Databases

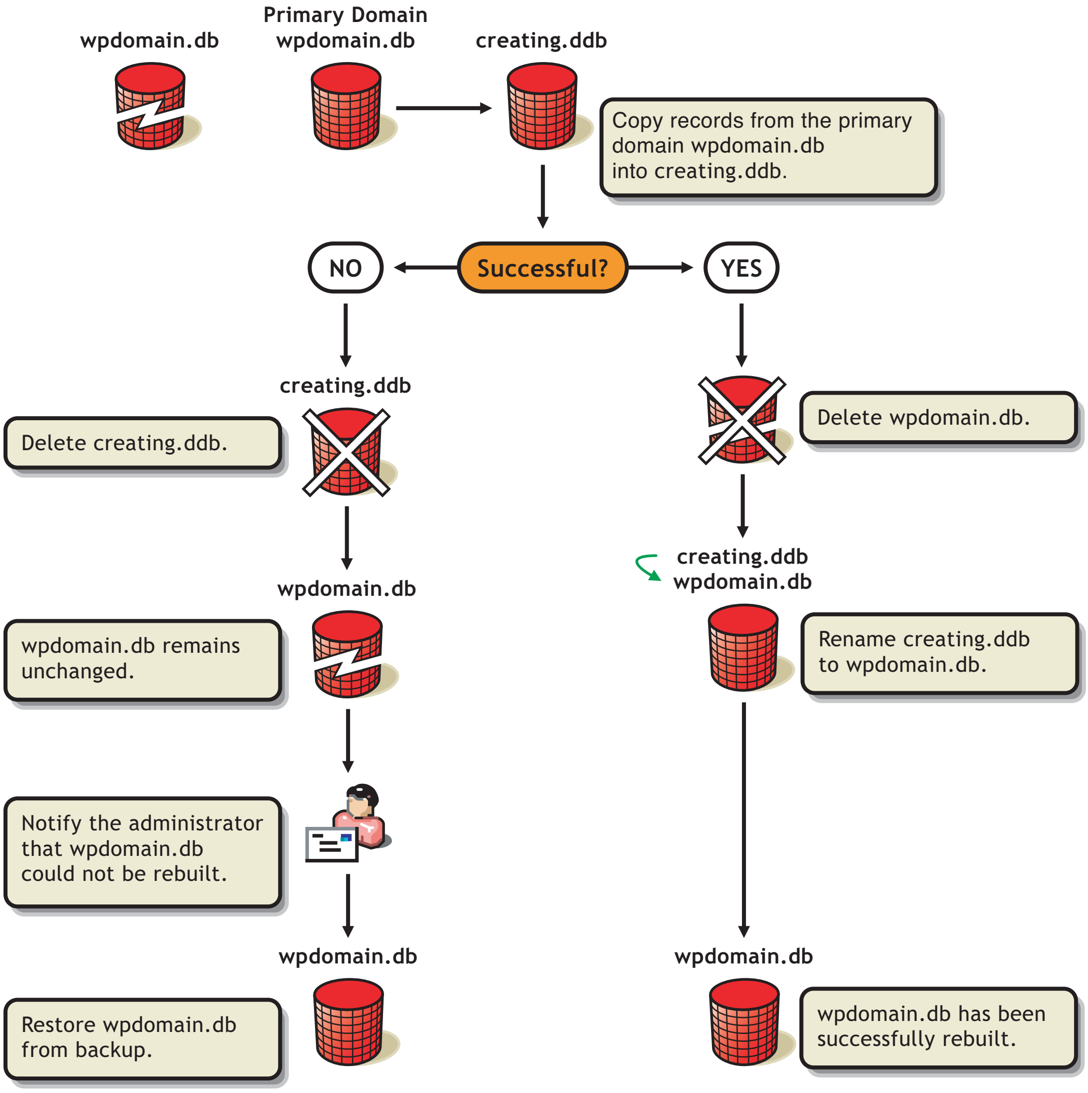
In addition to correcting the physical problems resolved by the database recover process, the rebuild process updates user and object information in a domain database (wpdomain.db) or post office database (wphost.db). However, the process requires that no users or GroupWise agents (MTA or POA) have access to the database during the rebuild process.

You should rebuild a domain or post office database if you encounter any of the following conditions:

- Objects are not being replicated between domains.
- The agent that writes to the database went down unexpectedly.
- The server where the database resides went down unexpectedly.
- You receive an administrative message informing you that an internal database error has occurred or there is database damage and you think there might be data loss.
- You ran the recover database process and received a notification of data loss.

When you rebuild a secondary domain database, information is retrieved from the primary domain. When you rebuild a post office database, information is retrieved from the domain it belongs to.

During the rebuild process, a backup of the domain or post office database is created as well as a new wpdomain.db or wphost.db. The records from the primary domain database are copied into the new wpdomain.db. There should not be any data loss. When the rebuild process is complete, the temporary database and the backup database are deleted.


wpdomain.db
Primary Domain
wpdomain.db
creating.ddb
Copy records from the primary domain wpdomain.db into creating.ddb.
NO
Successful?
YES
creating.ddb
Delete creating.ddb.
Delete wpdomain.db.
creating.ddb
wpdomain.db
wpdomain.db
wpdomain.db remains unchanged.
Rename creating.ddb to wpdomain.db.
Notify the administrator that wpdomain.db could not be rebuilt.
wpdomain.db
wpdomain.db
Restore wpdomain.db from backup.
wpdomain.db has been successfully rebuilt.

To rebuild a database:

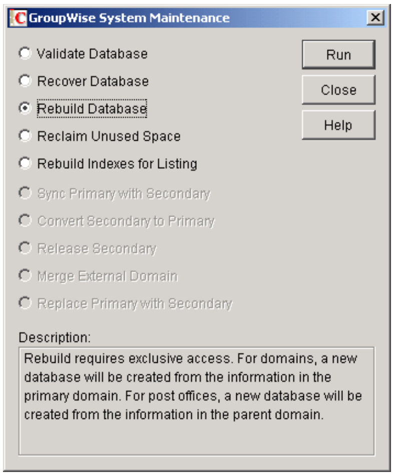
1 All GroupWise agents that might access the database must be stopped during the rebuild. See "Stopping the MTA" on page 609 and "Stopping the POA" on page 480.

2 If you are rebuilding a post office database, all users should exit and you should disable the post office before the rebuild. See "Disabling a Post Office" on page 183.

3 Make sure you have sufficient disk space for the copy of the database that is created during the rebuild process.

4 In ConsoleOne, browse to and select the Domain object or Post Office object where you want to rebuild the database.

5 Click Tools > GroupWise Utilities > System Maintenance.


GroupWise System Maintenance
○ Validate Database
○ Recover Database
● Rebuild Database
○ Reclaim Unused Space
○ Rebuild Indexes for Listing
○ Sync Primary with Secondary
○ Convert Secondary to Primary
○ Release Secondary
○ Merge External Domain
○ Replace Primary with Secondary
Run
Close
Help

Description:

Rebuild requires exclusive access. For domains, a new database will be created from the information in the primary domain. For post offices, a new database will be created from the information in the parent domain.

6. Click Rebuild Database > Run.
7. When prompted, make sure the Path to Database is correct. If an incorrect path is displayed, browse to and select the path to the database being rebuilt. Click OK.

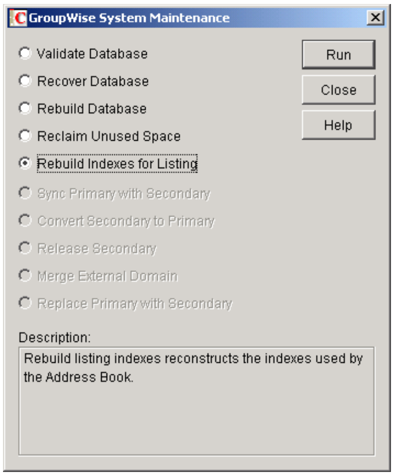
Rebuilding Database Indexes

Each domain database (wpdomain.db) and post office database (wphost.db) contains three indexes that are used to determine the order of the Address Book: the system index, the domain index, and the post office index. When you display the system Address Book, the system index is used. When you display a domain-level Address Book, the domain index is used, and when you display the Address Book for a post office, the post office index is used.

The GroupWise client uses the post office database to list users. If you are in the GroupWise client and the indexes for listing system, domain, and post office users are different than the domain database indexes, you should rebuild the post office database indexes. The most common cause of incorrect indexes in a post office is that the post office database was closed when you set up the list information.

To rebuild a database index:

1. Make sure you have administrative rights to the database whose indexes you are rebuilding.
2. In ConsoleOne, browse to and select the Domain object or Post Office object where you want to rebuild the database index.
3. Click Tools > GroupWise Utilities > System Maintenance.



GroupWise System Maintenance

○ Validate Database
○ Recover Database
○ Rebuild Database
○ Reclaim Unused Space
● Rebuild Indexes for Listing
○ Sync Primary with Secondary
○ Convert Secondary to Primary
○ Release Secondary
○ Merge External Domain
○ Replace Primary with Secondary

Description:
Rebuild listing indexes reconstructs the indexes used by the Address Book.

4 Select Rebuild Indexes for Listing, then click Run.

5 When prompted, make sure the Path to Database is correct. If an incorrect path is displayed, browse to and select the path to the database being whose indexes are being rebuilt. Click OK.

27 Maintaining User/Resource and Message Databases

It is sometimes necessary to perform maintenance tasks on user and resource databases (user*xxx*.db) and message databases (msg*nn*.db). The frequency depends on the reliability of your network and your own experience of how often problems are likely to occur. The following tasks help you maintain the integrity of your user and message databases.

- "Analyzing and Fixing User and Message Databases" on page 353
- "Performing a Structural Rebuild of a User Database" on page 355
- "Re-creating a User Database" on page 356

NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

To further protect your GroupWise® users against loss of mailbox contents, see Chapter 31, "Backing Up GroupWise Databases," on page 375 and Chapter 32, "Restoring GroupWise Databases from Backup," on page 379.

To ensure that the same information exists for users and messages throughout your GroupWise system, see "Synchronizing Individual Users or Resources" on page 363.

Analyzing and Fixing User and Message Databases

The Analyze/Fix option of Mailbox/Library Maintenance looks for problems and errors in user and resource databases (user*xxx*.db) and/or message databases (msg*nn*.db) and then fixes them if you select the Fix Problems option. You can analyze databases individually or you can analyze all user, resource, and/or message databases in one or more post offices.

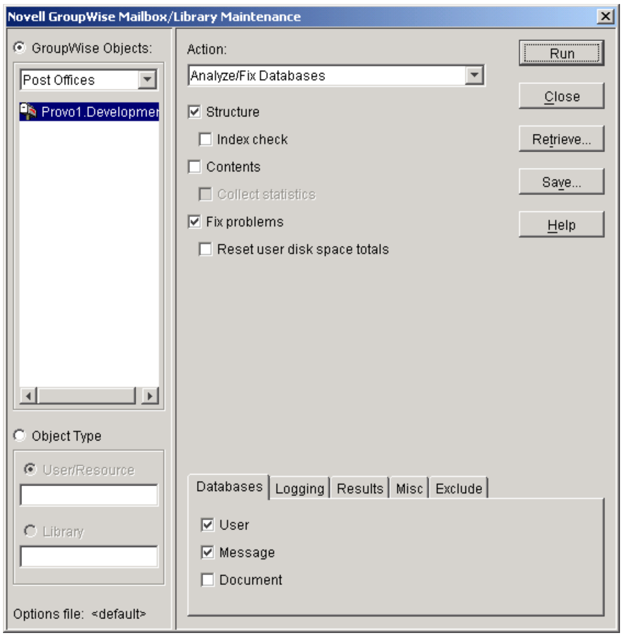
To analyze and repair user, resource, and/or message databases:

1. In ConsoleOne®, browse to and select one or more User or Resource objects to check individual users or resources.

   or

   Browse to and select one or more Post Office objects to check all user and/or message databases in the post office.

2. Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



● GroupWise Objects: Post Offices

Provo1.Developmer

○ Object Type

● User/Resource

○ Library

Options file: <default>

Action: Analyze/Fix Databases

☑ Structure

□ Index check

□ Contents

□ Collect statistics

☑ Fix problems

□ Reset user disk space totals

☑ User

☑ Message

□ Document

3 From the Action drop-down menu, select Analyze/Fix Databases.

4 Select from the following options:

Structure: When a user experiences a problem that is related to the user, message, or library databases, you should perform a structure check. The structure check verifies the integrity of the databases and reports the amount of space that could be recovered. If there is a structural problem, the databases are rebuilt with free space reclaimed.

Index Check: If you select Structure, you can also select Index Check. You should run an index check if a user tries to open a message and gets a read error, or when sent items that show a delivered status in the Properties window do not appear in the recipient's mailbox. An index check can be time-consuming.

Contents: The user databases (located in the ofuser directory) do not contain user messages. Messages are contained in the message databases under the ofmsg directory. However, the message databases do not contain the message attachments; these are located in the offiles directory. A contents check analyzes references to other items. For example, in the user database, Mailbox/Library Maintenance verifies that any referenced messages actually exist in the message database. In the message database, it verifies that any attachments that are referenced actually exist in the attachment directories.

Collect Statistics: If you selected Contents, the Collect Statistics option is available to collect and display statistics about the post office, such as the number of messages and appointments in the post office and the average number per user. In addition, you can display any user mailboxes that have more than a specified number of items. This can help determine if some users are using an excessive amount of disk space. If this is a problem, you might want to encourage users to delete unneeded items or to use the Archive feature in the GroupWise client to store messages on their local drives. You can also limit the amount of disk space each user can have. See "Managing Disk Space Usage in the Post Office" on page 171.

Fix Problems: This option tells Mailbox/Library Maintenance to fix any problems it finds. Otherwise, Mailbox/Library Maintenance will just report the problems.

Reset User Disk Space Totals: Recalculates the total disk space a GroupWise user is using by reading the selected user mailboxes and updating the poll record used for disk space management. Because disk space is user-specific, the program calculates the amount of disk space in use by the user in the user databases, in any of the message databases, and in the attachment directory. Disk space limitations do not take into account the disk space used in document libraries. This option is usually run if the user totals are not being reflected correctly.

5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

   "Databases" on page 396

   "Logging" on page 396

   "Results" on page 396

   "Misc" on page 397

   "Exclude" on page 397

   Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 397.

6 Click Run to perform the Analyze/Fix operation.

Analyze/Fix can also be run using the standalone GroupWise Check program. See "GroupWise Check" on page 391. It can also be scheduled to run on a regular basis by properly configuring the POA. See "Scheduling Database Maintenance" on page 467.

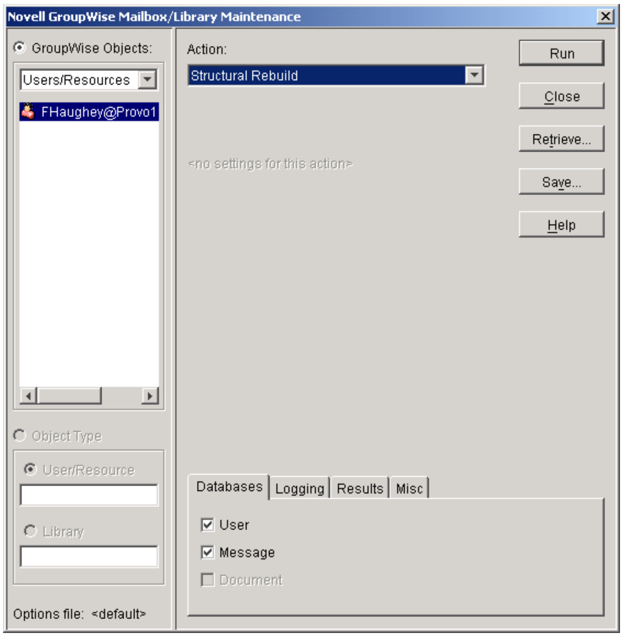
Performing a Structural Rebuild of a User Database

The Structural Rebuild option of Mailbox/Library Maintenance rebuilds the structure of a user or resource database (user*xxx*.db) and reclaims any free space. It does not re-create the contents of the database. If you need to recover database contents as well as structure, see "Re-creating a User Database" on page 356.

To rebuild a user database:

1 In ConsoleOne, browse to and select one or more User or Resource objects whose database needs to be rebuilt.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



● GroupWise Objects: Users/Resources

FHaughey@Provo1

○ Object Type

● User/Resource

○ Library

Options file: <default>

Action: Structural Rebuild

<no settings for this action>

☑ User

☑ Message

☐ Document

3 From the Action drop-down list, select Structural Rebuild.

4 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

"Databases" on page 396

"Logging" on page 396

"Results" on page 396

"Misc" on page 397

Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 397.

5 Click Run to perform a structural rebuild of the user database.

Re-creating a User Database

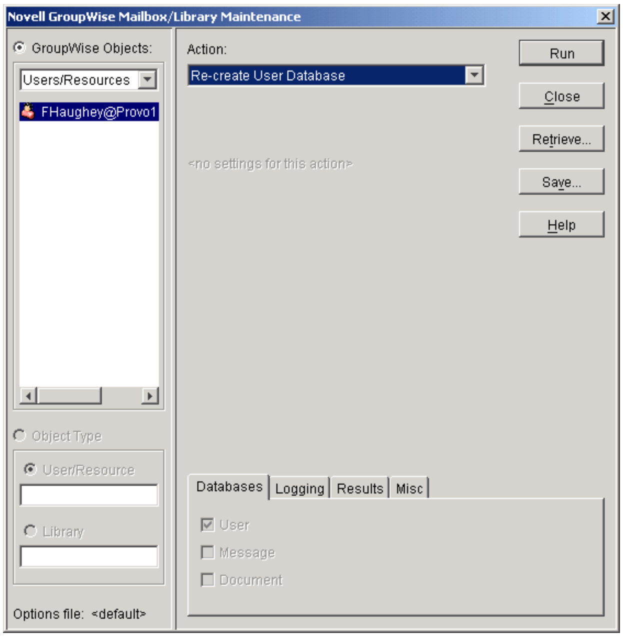
The Re-create User Database option of Mailbox/Library Maintenance will rebuild a user or resource database (user*xxx*.db) and recover any information it can. Some information is lost, such as the folder assignments.

You should never need to select this option for regular database maintenance. It is designed for severe problems, such as replacing a user database that has been accidentally deleted and for which you have no backup copy. Because folder assignments are lost, all items are placed into the Cabinet folder. The user must then reorganize all the items in his or her mailbox. Use of filters and searching can facilitate this process, but it is not a desirable experience. It is, however, preferable to losing everything.

To re-create a user database:

1 In ConsoleOne, browse to and select one or more User or Resource objects that need the user database re-created.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



● GroupWise Objects: Users/Resources

FHaughey@Provo1

Action: Re-create User Database

<no settings for this action>

○ Object Type

● User/Resource

○ Library

Options file: <default>

☑ User

□ Message

□ Document

3 From the Action drop-down list, select Re-create User Database.

4 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

“Databases” on page 396

“Logging” on page 396

“Results” on page 396

“Misc” on page 397

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 397.

5 Click Run to re-create the user database.

28 Maintaining Library Databases and Documents

GroupWise® Document Management Services (DMS) uses libraries as repositories for documents. For a review of library database structure, see "Library Databases" on page 342.

- "Analyzing and Fixing Databases for Libraries and Documents" on page 359
- "Analyzing and Fixing Library and Document Information" on page 360

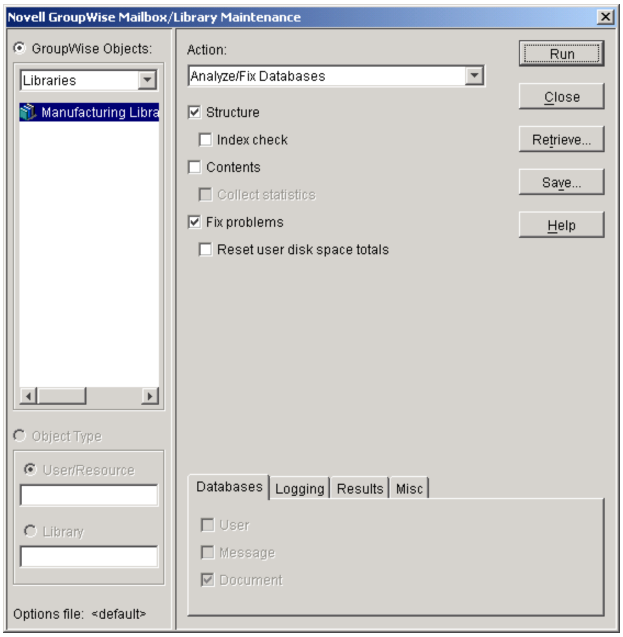
NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

Analyzing and Fixing Databases for Libraries and Documents

For libraries, the Analyze/Fix Databases option of Mailbox/Library Maintenance looks for problems and errors in library and document databases and then fixes them if you select the Fix Problems option.

To analyze and repair library and document databases:

1. In ConsoleOne®, browse to and select one or more Library objects.
2. Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



Novell GroupWise Mailbox/Library Maintenance

● GroupWise Objects: Libraries

Manufacturing Libra

○ Object Type

● User/Resource

○ Library

Options file: <default>

Action: Analyze/Fix Databases

☑ Structure

☐ Index check

☐ Contents

☐ Collect statistics

☑ Fix problems

☐ Reset user disk space totals

Databases | Logging | Results | Misc

☐ User

☐ Message

☑ Document

3. From the Action drop-down menu, select Analyze/Fix Databases.
4. Select from the following options:

Structure: When a user experiences a problem that is related to the library databases, you should perform a structure check. The structure check verifies the integrity of the databases and reports the amount of space that could be recovered. If there is a structural problem, the databases are rebuilt with free space reclaimed.

Index Check: If you select Structure, you can also select Index Check. An index check can be time-consuming.

Contents: The library database (located in the gwdms directory of the post office) does not contain documents. Documents are stored in the lib00*00-FF* directories. A contents check analyzes references from libraries to documents.

Collect Statistics: If you selected Contents, the Collect Statistics option is available to collect and display statistics about the library, such as the number and size of documents.

Fix Problems: This option tells Mailbox/Library Maintenance to fix any problems it finds. Otherwise, Mailbox/Library Maintenance will just report the problems.

5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

“Databases” on page 396

“Logging” on page 396

“Results” on page 396

“Misc” on page 397

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 397.

6 Click Run to perform the Analyze/Fix Databases operation on the library.

Analyze/Fix Databases can also be run using the standalone GroupWise Check program. See “GroupWise Check” on page 391. It can also be scheduled to run on a regular basis by properly configuring the POA. See “Scheduling Database Maintenance” on page 467.

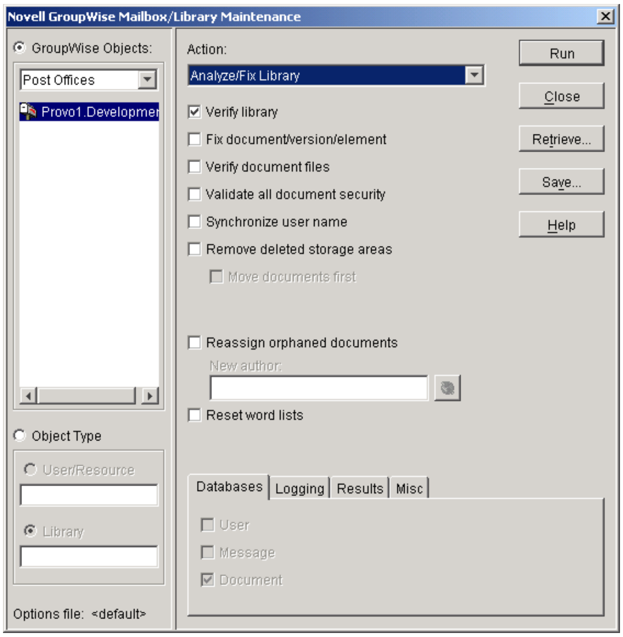
Analyzing and Fixing Library and Document Information

The Analyze/Fix Library option of Mailbox/Library Maintenance performs more library-specific functions that Analyze/Fix Databases. For all options except Verify Library, all documents in each of the selected library databases are checked. This can be a time-consuming process. Therefore, if you intend to select more than one of the Analyze/Fix Library options, you can save time by selecting each of them before clicking Run. This causes all selected options to be run against each document, which is faster than running each option individually against all documents.

To validate library databases:

1 In ConsoleOne, browse to and select one or more Post Office objects where you want to validate libraries.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



● GroupWise Objects:

Post Offices

Provo1.Developmen

○ Object Type

○ User/Resource

● Library

Options file: <default>

Action: Analyze/Fix Library

☑ Verify library

☐ Fix document/version/element

☐ Verify document files

☐ Validate all document security

☐ Synchronize user name

☐ Remove deleted storage areas

☐ Move documents first

☐ Reassign orphaned documents

New author:

☐ Reset word lists

☐ User

☐ Message

☑ Document

3 From the Action drop-down menu, select Analyze/Fix Library.

4 Select from the following options:

Verify Library: This is a post office-level check. It verifies that all libraries are on the libraries list. It also checks the schema and guarantees its integrity. If there is a problem with the schema, it resets to a default schema to reclaim any missing items. For example, if you deleted the Document Type property, you could recover it using this option.

Fix Document/Version/Element: This performs an integrity check to verify the following:

- Each document has one or more versions linked to it.
- Each version has one or more elements linked to it.
- All versions are linked to a document.
- All elements are linked to a version.

If there are any missing links, the missing documents or versions are created from the information contained in the existing version or element for which the link is missing. For example, if a version is found that shows no link to a document, a document is created from the information contained in the version and the link is reestablished. Of course, any information in the lost document that might have been newer than the information contained in the old version is lost.

Verify Document Files: This determines if the BLOB exists for a document and the document is accessible. If not, an error is logged for that document. The log message does not indicate why a file is missing or inaccessible. You can recover a file by restoring it from backup.

Possible errors that would be logged include:

- If the file system on the network becomes corrupted, this will tell you which documents cannot be opened or which BLOB files are missing.
- If a file was marked by someone as Read Only or Hidden, this option would log an error that the file is inaccessible.

Validate All Document Security: This option validates document security for the Author, Creator and Security (document sharing) fields. The validation replaces the results of selecting the Validate Author/Creator Security option, and is more thorough. Therefore, you only need to select one option or the other.

Synchronize User Name: The Author and Creator fields display users' full names, not unique IDs. If a user's name is changed, such as for marriage, this option verifies that the user's name on document and version records is the same as the user's current display name. In other words, the Author and Creator fields in documents and versions are updated to the user's newer name.

Remove Deleted Storage Areas: When you delete a document storage area in the Storage Areas page of a library's details dialog box, the document storage area and the documents stored there remain on the system. Deleting the storage area from the library only means that new documents will not be stored there. The documents there will continue to be available to users.

If you want to also remove the document storage area from the system, you have two options: delete the storage area and its documents, or first move the documents and then delete the storage area. The first option is not advisable, but exists so that if you have moved all of the documents that can be moved, but some corrupted documents are left behind, you can force the document storage area to be deleted.

You should normally check the Move Documents First box so that users will continue to have access to those documents from a different document storage area. With this option, all BLOBs in the library are checked to see which documents are in the area being deleted.

Reassign Orphaned Documents: Documents can occasionally become orphaned (unattached to a user). For example, this can happen when a user leaves your organization and the user object is removed. All documents belonging to that user are no longer available in GroupWise searches and cannot be accessed by anyone (document security is controlled by the user listed in the Author and Creator fields). This option lets you reassign these documents to another user. You must select a new author from the browser menu after checking this option. The new author you designate will have access to all orphaned documents in this library.

Reset Word Lists: Documents stored in a library are indexed and inserted into a generated word list. This allows users to search for a document by keywords as well as any word contained within a document. The document library word list might become outdated and if this occurs, the word list must be regenerated. This option allows the program to regenerate the document library word list the next time an index operation is performed.

5. Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

   "Databases" on page 396

   "Logging" on page 396

   "Results" on page 396

   "Misc" on page 397

   Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 397.

6. Click Run to perform the Analyze/Fix Library operation.

Analyze/Fix Library can also be run using the standalone GroupWise Check program. See "GroupWise Check" on page 391. It can also be scheduled to run on a regular basis by properly configuring the POA. See "Scheduling Database Maintenance" on page 467.

29 Synchronizing Database Information

In general, synchronization of object information throughout your GroupWise® system occurs automatically. Whenever you add, delete, or modify a GroupWise object, the information is automatically replicated to all appropriate databases. Ideally, each domain database (wpdomain.db) in your system contains original records for all objects it owns and accurately replicated records for all objects owned by other domains. However, because unavoidable events such as power outages and hardware problems can disrupt network connectivity, information in various databases might get out of sync.

If you think you have a synchronization problem, especially soon after adding, deleting, or modifying objects, it is wise to check Pending Operations to make sure your changes have been processed. See "Pending Operations" on page 51. When waiting for replication to take place, patience is a virtue.

When information differs between the original record and a replicated record, the original record is considered correct. If you perform synchronization from the owning domain, the owning domain notifies the primary domain of the correct information, then the primary domain broadcasts the correct information to all secondary domains. Therefore, the best place to perform synchronization is from the domain that owns the object that is out of sync. The next best place to perform synchronization is from the primary domain, because the primary domain sends a request to the owning domain for the correct information, then broadcasts the correct information to all secondary domains.

Any GroupWise object can be synchronized:

- "Synchronizing Individual Users or Resources" on page 363
- "Synchronizing a Post Office" on page 364
- "Synchronizing a Secondary Domain" on page 365
- "Synchronizing the Primary Domain from a Secondary Domain" on page 366

Synchronizing Individual Users or Resources

Most often, you will notice a synchronization problem when a user has trouble sending a message. Symptoms include:

- The sender receives a "user is undeliverable" message.
- A new user or resource created in ConsoleOne® does not appear in the Address Book in some or all post offices.
- User or resource information is incorrect in the Address Book but correct in ConsoleOne.
- A user or resource is listed in the Address Book as belonging to one post office but actually belongs to another.

To synchronize individual User and/or Resource objects:

1. In ConsoleOne, connect to the domain that owns the users and/or resources. See "Connecting to a Domain" on page 123.

   or

   Connect to the primary domain.

2. Browse to and right-click one or more User or Resource objects to synchronize, then click Properties.

3. Make sure the correct information appears on the object's Identification page, then click Cancel.

4. Repeat Step 2 and Step 3 for each user or resource you need to synchronize.

5. Select each User or Resource object, then click Tools > GroupWise Utilities > Synchronize.

6. When you are asked whether to proceed, click Yes.

   Current, correct information will then be replicated throughout your GroupWise system.

   If many User or Resource objects are being synchronized, you can check progress by viewing pending operations. See "Pending Operations" on page 51.

   After synchronization is complete, you can verify that it was successful by checking the synchronized objects in Address Books and several post offices in your GroupWise system.

If there are indications that a large number of User or Resource objects need to be synchronized, rebuilding the post office database (wphost.db) can be preferable to synchronizing individual objects. However, this process requires exclusive access to the post office database. See "Rebuilding Domain or Post Office Databases" on page 349.

Occasionally, GroupWise user information can get out of sync with Novell® eDirectory™ user information. This requires a different type of synchronization process. See "Using eDirectory User Synchronization" on page 598.

Synchronizing a Post Office

If information for a particular post office does not display the same throughout your GroupWise system, you can synchronize the post office.

1. In ConsoleOne, connect to the domain that owns the post office. See "Connecting to a Domain" on page 123.

   or

   Connect to the primary domain.

2. Browse to and right-click the Post Office object to synchronize, then click Properties.

3. Make sure the correct information appears on the post office Identification page, then click Cancel.

4. Select the Post Office object, then click Tools > GroupWise Utilities > Synchronize.

5. When you are asked whether to proceed, click Yes.

   Current, correct post office information will then be replicated throughout your GroupWise system.

   After synchronization is complete, you can verify that it was successful by checking the post office information when connected to different domains in your GroupWise system.

See also "Rebuilding Domain or Post Office Databases" on page 349.

Synchronizing a Library

If information for a library does not display the same throughout your GroupWise system, you can synchronize the library.

1 In ConsoleOne, connect to the domain that owns the library. See "Connecting to a Domain" on page 123.

or

Connect to the primary domain.

2 Browse to and right-click the Library object to synchronize, then click Properties.

3 Make sure the correct information appears on the library Identification page, then click Cancel.

4 Select the Library object, then click Tools > GroupWise Utilities > Synchronize.

5 When you are asked whether to proceed, click Yes.

Current, correct library information will then be replicated throughout your GroupWise system.

After synchronization is complete, you can verify that it was successful by checking the library information when connected to different domains in your GroupWise system.

See also "Analyzing and Fixing Library and Document Information" on page 360.

Synchronizing a Secondary Domain

If information for a particular secondary domain does not display the same throughout your GroupWise system, you can synchronize the secondary domain.

1 In ConsoleOne, connect to the primary domain. See "Connecting to a Domain" on page 123.

2 If there is any doubt about the correctness of that secondary domain's information as stored in the primary domain database, synchronize the primary domain with the secondary domain before proceeding. See "Synchronizing the Primary Domain from a Secondary Domain" on page 366.

3 Browse to and right-click the Domain object to synchronize, then click Properties.

4 Make sure the correct information appears on the domain Identification page, then click Cancel.

5 Select the Domain object, then click Tools > GroupWise Utilities > Synchronize.

6 When you are asked whether to proceed, click Yes.

Current, correct domain information for the secondary domain will then be replicated throughout your GroupWise system.

After synchronization is complete, you can verify that it was successful by checking the domain information when connected to different domains in your GroupWise system.

See also "Rebuilding Domain or Post Office Databases" on page 349.

Synchronizing the Primary Domain from a Secondary Domain

Information about a secondary domain stored in the secondary domain database is considered more current and correct than information about that secondary domain stored in the primary domain database. If the primary domain database contains out-of-date information, you can synchronize the primary domain from the secondary domain.

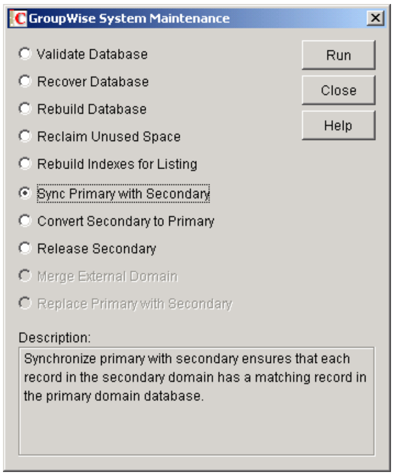
When you synchronize the primary domain database from a secondary domain database, any records the secondary domain owns, such as post offices or users added to the secondary domain, are replicated from the secondary domain database to the primary domain database.

To synchronize the primary domain from a secondary domain:

1 You must have administrative rights to the primary domain directory and the secondary domain directory from which the primary domain is being synchronized.

2 In ConsoleOne, browse to and select the Domain object of the secondary domain whose database you want to use to synchronize the primary domain database.

3 Click Tools > GroupWise Utilities > System Maintenance.



GroupWise System Maintenance

○ Validate Database
○ Recover Database
○ Rebuild Database
○ Reclaim Unused Space
○ Rebuild Indexes for Listing
● Sync Primary with Secondary
○ Convert Secondary to Primary
○ Release Secondary
○ Merge External Domain
○ Replace Primary with Secondary

Description:
Synchronize primary with secondary ensures that each record in the secondary domain has a matching record in the primary domain database.

4 Select Sync Primary with Secondary, then click Run.

5 When prompted, make sure the Path to Database is correct. If an incorrect path is displayed, browse to and select the path to the database being validated. Click OK.

To make sure the primary domain database is totally up-to-date, repeat the procedure for each secondary domain in your system.

30 Managing Database Disk Space

One of the most common maintenance issues in a growing system is running out of disk space. In addition to sending messages, users tend to use GroupWise® for all sorts of communication, such as transferring large files. Library documents created with Document Management Services (DMS) can use huge amounts of disk space. Archived library documents can also quickly use up disk space assigned to the post office, where space is usually limited.

You should let your users know about the archive and auto-delete features of GroupWise mail, or set client options in ConsoleOne® to automatically archive or delete. See Chapter 74, "Setting Defaults for the GroupWise Client Options," on page 973.

- "Gathering Mailbox Statistics" on page 367
- "Reducing the Size of User and Message Databases" on page 369
- "Reclaiming Disk Space in Domain and Post Office Databases" on page 370
- "Reducing the Size of Libraries and Document Storage Areas" on page 371

See also "Managing Disk Space Usage in the Post Office" on page 171.

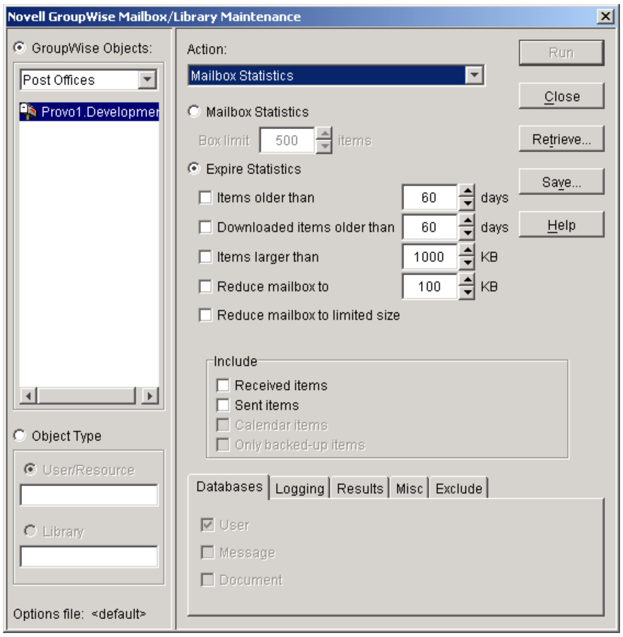
Gathering Mailbox Statistics

If you have some users who don't like to throw anything away, you might want to monitor the size of their mailboxes and, where appropriate, suggest voluntary cleanup. You can assess e-mail retention by the number of messages, age of messages, or size of user databases.

The Mailbox Statistics option in Mailbox/Library Maintenance collects and displays statistics about the post office, such as the number of messages and appointments in the post office and the average number per user. It is valid only for user databases. In addition, you can display any user mailboxes that have more than a specified number of items. This can help determine which users might be using an excessive amount of file server disk space.

To gather mailbox statistics:

1. In ConsoleOne, browse to and select one or more User or Resource objects or one or more Post Office objects.
2. Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



● GroupWise Objects:

Post Offices

Provo1.Developmen

○ Object Type

● User/Resource

○ Library

Options file: <default>

Action: Mailbox Statistics

○ Mailbox Statistics

Box limit 500 items

● Expire Statistics

□ Items older than 60 days

□ Downloaded items older than 60 days

□ Items larger than 1000 KB

□ Reduce mailbox to 100 KB

□ Reduce mailbox to limited size

Include

□ Received items

□ Sent items

□ Calendar items

□ Only backed-up items

☑ User

□ Message

□ Document

3 From the Action drop-down menu, select Mailbox Statistics.

4 Select Mailbox Statistics.

Mailbox Statistics: Enter a maximum number of items. You will see a report showing each user whose mailbox has more items in it than the number you specify.

or

Select Expire Statistics.

Expire Statistics: Select one of the following:

- **Items Older Than:** Shows how many items are older than the number of days you specify.
- **Downloaded Items Older Than:** Shows how many items have been downloaded to users' GroupWise Caching or Remote mailboxes that are older than the number of days you specify. This does not include items that have been downloaded to non-GroupWise mailboxes (for example, POP and IMAP accounts).
- **Items Larger Than:** Shows how many items are larger than the size you specify.
- **Reduce Mailbox To:** Shows how many items need to be expired before the mailbox would be reduced to the size you specify. Older, larger items are expired before newer, smaller items.
- **Reduce Mailbox to Limited Size:** Shows how many items need to be expired before the mailbox is the size specified using the Disk Space Management feature under Client Options, as described in "Setting Mailbox Size Limits" on page 172.

5 In the Include box, select Received Items, Sent Items, Calendar Items, and/or Only Backed-Up Items to specify the types of items to gather statistics for.

6 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

"Databases" on page 396

"Logging" on page 396

"Results" on page 396

"Misc" on page 397

"Exclude" on page 397

Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 397.

By default, the mailbox statistics are sent to the domain administrator, as designated in "Notifying the Domain Administrator" on page 632.

7 If you want to send the statistics to one or more other users, click Results, select Individual Users, specify the e-mail addresses in the users in the CC line, then click Message if you want to include explanatory text.

8 Click Run to gather the mailbox statistics and e-mail the results to the specified users.

Reducing the Size of User and Message Databases

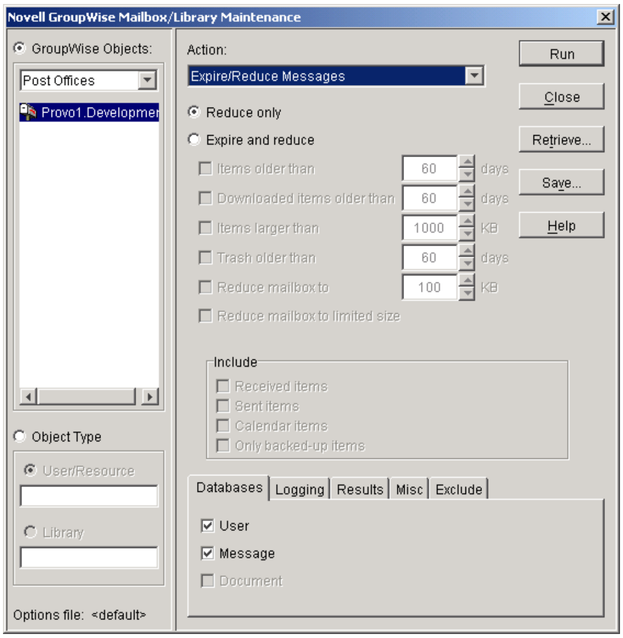
The Expire/Reduce Messages option of Mailbox/Library Maintenance eliminates expired messages and reclaims any free space in the database. You can expire/reduce messages for one or more users or resources, or for all users and resources in one or more post offices. You should inform users before you run this process so they have a chance to archive or delete messages.

1 In ConsoleOne, browse to and select one or more User or Resource objects to expire/reduce messages for the selected users and resources.

or

Browse to and select one or more Post Office objects to expire/reduce messages for all users and resources in each selected post office.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



Novell GroupWise Mailbox/Library Maintenance

● GroupWise Objects: Post Offices

Provo1.Developmen

○ Object Type

● User/Resource

○ Library

Options file: <default>

Action: Expire/Reduce Messages

● Reduce only

○ Expire and reduce

□ Items older than 60 days

□ Downloaded items older than 60 days

□ Items larger than 1000 KB

□ Trash older than 60 days

□ Reduce mailbox to 100 KB

□ Reduce mailbox to limited size

Include

□ Received items

□ Sent items

□ Calendar items

□ Only backed-up items

Databases

☑ User

☑ Message

□ Document

3 From the Action drop-down menu, select Expire/Reduce Messages.

4 Click Reduce Only to delete items that have already expired.

or

Click Expire and Reduce.

Expire and Reduce: Select one or more of the following:

- **Items Older Than:** Expires items that are older than the number of days you specify.
- **Downloaded Items Older Than:** Expires items that have been downloaded to users' GroupWise Caching or Remote mailboxes that are older than the number of days you specify. It does not expire items that have been downloaded to non-GroupWise mailboxes (for example, POP and IMAP accounts).
- **Items Larger Than:** Expires items that are larger than the size you specify.
- **Trash Older Than:** Expires items in the Trash that are older than the number of days you specify.
- **Reduce Mailbox To:** Expires items until the mailbox is reduced to the size you specify. Older, larger items are expired before newer, smaller items.
- **Reduce Mailbox to Limited Size:** Expires items until the mailbox is the size specified using the Disk Space Management feature under Client Options, as described in "Setting Mailbox Size Limits" on page 172.

5. In the Include box, select Received Items, Sent Items, Calendar Items, and/or Only Backed-Up Items. You might want to notify users of the types of items that will be deleted.
6. Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

   "Databases" on page 396
   "Logging" on page 396
   "Results" on page 396
   "Misc" on page 397
   "Exclude" on page 397

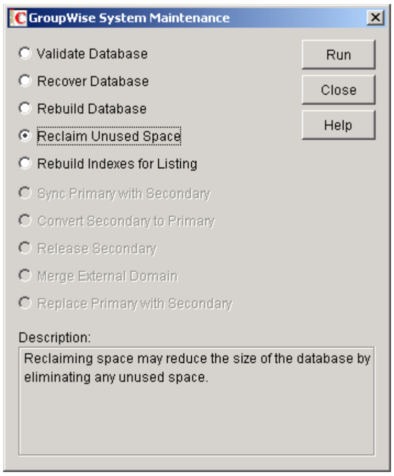
   Selected options can be saved for repeated use. See "Saving Mailbox/Library Maintenance Options" on page 397.
7. Click Run to perform the Expire/Reduce Messages operation.

For additional disk space management assistance, see "Managing Disk Space Usage in the Post Office" on page 171.

Reclaiming Disk Space in Domain and Post Office Databases

As you add information to your system, the domain databases (wpdomain.db) and post office databases (wphost.db) increase in size. If you delete information, the space created in the databases for the information is not immediately recovered. GroupWise will use the free space before requiring more disk space; however, if you have deleted a large amount of information, you might want to reclaim unused database space. If you have frequent changes to your users, especially deletions, you should occasionally reclaim disk space.

1. In ConsoleOne, browse to and select the Domain object or Post Office object where you want to reclaim disk space.
2. Click Tools > GroupWise Utilities > System Maintenance.



○ Validate Database
○ Recover Database
○ Rebuild Database
● Reclaim Unused Space
○ Rebuild Indexes for Listing
○ Sync Primary with Secondary
○ Convert Secondary to Primary
○ Release Secondary
○ Merge External Domain
○ Replace Primary with Secondary

Description:
Reclaiming space may reduce the size of the database by eliminating any unused space.

3 Select Reclaim Unused Space, then Run.

4 When prompted, make sure the Path to Database is correct. If an incorrect path is displayed, browse to and select the path to the database where you want to reclaim disk space. Click OK.

Reducing the Size of Libraries and Document Storage Areas

The amount of disk space you allow at each post office for your library databases varies according to the GroupWise features they use.

If you are using GroupWise Document Management Services, you will need to determine storage requirements for your documents. If you feel your current disk space usage by documents is not representative of your long-term requirements, you can estimate the disk space users will need for documents by multiplying an average document size by the average number of documents per user by the total number of users in the post office.

For example, the typical document size is 50 KB. Each user owns about 50 documents and there are 100 users on your post office.

Sample Calculation:

```
   50 KB (document size)
x  50 documents (per user)
x 100 users
-----
  2.5 GB of disk space
```

Be sure to allow your libraries room to grow.

When room to grow is no longer available, the following tasks help you make the best use of available disk space:

- "Archiving and Deleting Documents" on page 372
- "Deleting Activity Logs" on page 373

See also "Backing Up and Restoring Archived Documents" on page 328.

Archiving and Deleting Documents

Documents can be archived, retained indefinitely, or simply deleted. The document type property determines a document's disposition (archive, delete, or retain). The document life property determines when it can be archived or deleted. When you run the Archive/Delete Documents option of Mailbox/Library Maintenance, documents in the selected libraries that have reached their document life dates are either deleted or archived.

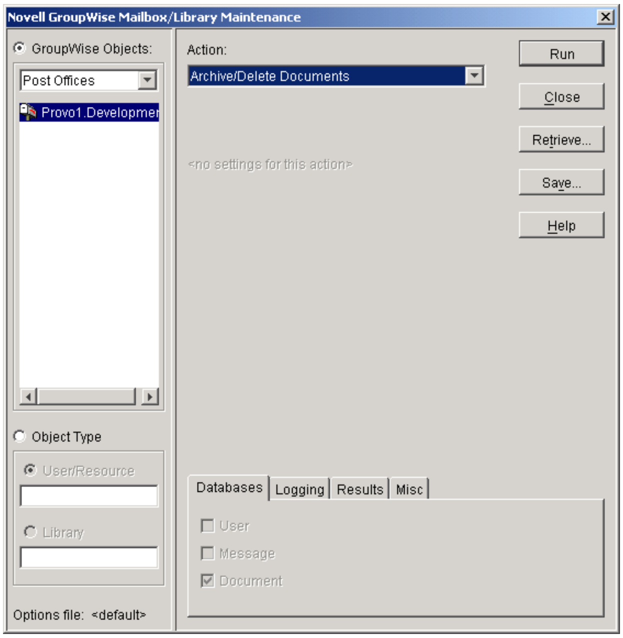
Documents that have reached their document life and been marked for deletion in the document type are simply deleted from the library, after which the document and its property information can no longer be found by any search. You can recover deleted documents from database backups.

When documents are archived, their BLOBs are moved to archive directories. These directories are named ar*nnnnnn* (where *nnnnnn* is an incremented integer with leading zeros), and are automatically created as needed. They are sometimes referred to as archive sets. The archive directories are located at *post_office_directory*\gwdms\lib*01-FF*\archive. When a document is archived, GroupWise determines if the document BLOB will fit in the current archive directory. If the BLOB will not fit, another archive directory is created and the BLOB is archived there.

To archive/delete documents from one library or all libraries in the selected post offices:

1 In ConsoleOne, select one or more Library objects or Post Office objects for the documents you want to archive/delete.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



Novell GroupWise Mailbox/Library Maintenance

● GroupWise Objects: Post Offices

Provo1.Developmer

○ Object Type

Action: Archive/Delete Documents

<no settings for this action>

Options file: <default>

3 From the Action drop-down menu, select Archive/Delete Documents.

4 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

"Databases" on page 396

"Logging" on page 396

"Results" on page 396

"Misc" on page 397

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 397.

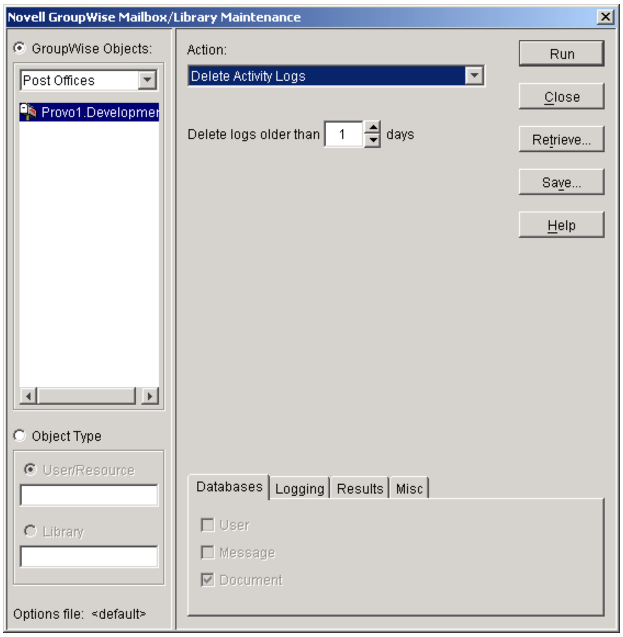
5 Click Run to perform the Archive/Delete Documents operation.

Deleting Activity Logs

To free up disk space by deleting the activity logs for one or more libraries:

1 In ConsoleOne, select one or more Library objects or Post Office object where you want to delete activity logs.

2 Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.



Novell GroupWise Mailbox/Library Maintenance

● GroupWise Objects: Post Offices

Provo1.Developmer

○ Object Type

Action: Delete Activity Logs

Delete logs older than 1 days

☑ Document

Options file: <default>

3 From the Action drop-down menu, select Delete Activity Logs.

4 Enter the number of days in the Delete Activity Logs Older Than field. The default is 60 days.

5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

“Databases” on page 396
“Logging” on page 396
“Results” on page 396
“Misc” on page 397

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 397.

6 Click Run to delete unneeded activity logs.

31 Backing Up GroupWise Databases

You should back up GroupWise® databases regularly so that if a database sustains damage that cannot be repaired using the GroupWise database maintenance tools, you can still recover with minimum data loss.

- "Backing Up a Domain" on page 375
- "Backing Up a Post Office" on page 375
- "Backing Up a Library and Its Documents" on page 376
- "Backing Up Individual Databases" on page 377

Backing Up a Domain

All critical domain-level information is stored in the domain database (wpdomain.db).

On NetWare, use a Target Service Agent (GWTSA or TSAFS) with a supported backup program or other backup software of choice to back up each domain database to a secure location. For details about how to use a Target Service Agent, see "Target Service Agents" on page 398.

On Linux and Windows, use your backup software of choice to back up each domain database to a secure location. For a list of compatible products, see the Partner Product Guide (http://www.novell.com/partnerguide). You can also use the GroupWise Database Copy utility (DBCopy) and the GroupWise Time Stamp utility (GWTMSTMP) to assist with backups. For details about how to use these utilities, see "Standalone Database Maintenance Programs" on page 391. If your backup software cannot handle open files, stop the MTA for the domain while the backup of the domain database takes place.

See also "Restoring a Domain" on page 379.

Backing Up a Post Office

Critical post office-level information is stored in many different databases. The table below summarizes the databases and their locations:

Database	Location
wphost.db	\post_office_directory
ngwguard.db	\post_office_directory
msg*nn*.db	\post_office_directory\ofmsg
user*xxx*.db	\post_office_directory\ofuser
pu*xxxxx*.db	\post_office_directory\ofuser

Database	Location
*.idx and *.inc	*post_office_directory*\ofuser\index
fd*0-F6*	*post_office_directory*\offiles
dmsh.db	*post_office_directory*\gwdms
dm*xxnn01-FF*.db	*post_office_directory*\gwdms\lib00*00-FF*
fd*0-FF*	*post_office_directory*\gwdms\lib00*00-FF*\docs
*.idx and *.inc	*post_office_directory*\gwdms\lib00*00-FF*\index

To view a post office directory structure diagram, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

On NetWare, use a Target Service Agent (GWTSA or TSAFS) with a supported backup program or other backup software of choice to regularly back up all databases in each post office to a secure location. For details about how to use a Target Service Agent, see "Target Service Agents" on page 398.

On Linux and Windows, use your backup software of choice to back up each post office to a secure location. For a list of compatible products, see the Partner Product Guide (http://www.novell.com/partnerguide). You can also use the GroupWise Database Copy utility (DBCopy) and the GroupWise Time Stamp utility (GWTMSTMP) to assist with backups. For details about how to use these utilities, see "Standalone Database Maintenance Programs" on page 391.

See also "Restoring a Post Office" on page 379.

Backing Up a Library and Its Documents

If the document storage area for a library is physically located in a post office, the library and documents are backed up along with the rest of the data in the post office. However, document storage areas are frequently located outside of the post office directory structure due to disk space considerations. Therefore, remote document storage areas must be backed up separately. A post office can have multiple libraries and each library can have multiple document storage areas, so make sure you have identified all document storage areas in your library/document backup procedure.

On NetWare, use a Target Service Agent (GWTSA or TSAFS) with a supported backup program or other backup software of choice to back up document storage areas. For details about how to use a Target Service Agent, see "Target Service Agents" on page 398.

On Linux and Windows, use your backup software of choice to back up each document storage area to a secure location. For a list of compatible products, see the Partner Product Guide (http://www.novell.com/partnerguide).

After you have initially performed a full backup of your document storage areas, you can perform incremental backups by backing up to the same location to shorten the backup process.

To ensure consistency between the backups of post office databases and document storage areas:

1. Back up your document storage areas.
2. Back up the post office. See "Backing Up a Post Office" on page 375.

3. Perform an incremental backup of your document storage areas to pick up all new documents and document modifications that occurred while backing up the post office.

You should need to restore data in a document storage area only if files have been damaged or become inaccessible due to a hard disk failure.

See also "Restoring a Library" on page 380.

Backing Up Individual Databases

If you need to back up individual databases separately from backing up a post office, you can use your backup software of choice.

See also "Restoring an Individual Database" on page 380.

32 Restoring GroupWise Databases from Backup

Database damage can usually be repaired using the database maintenance tools provided with GroupWise®. Only very occasionally should you need to restore databases from backup.

- "Restoring a Domain" on page 379
- "Restoring a Post Office" on page 379
- "Restoring a Library" on page 380
- "Restoring an Individual Database" on page 380
- "Restoring Deleted Mailbox Items" on page 381
- "Recovering Deleted GroupWise Accounts" on page 384

Restoring a Domain

Typically, damage to the domain database (wpdomain.db) can be repaired using the database maintenance tools provided in ConsoleOne®. See Chapter 26, "Maintaining Domain and Post Office Databases," on page 345.

If damage to the domain database is so severe that rebuilding the database is not possible:

1. Stop the MTA for the domain. See "Stopping the MTA" on page 609.
2. On NetWare, use a Target Service Agent (GWTSA of TSAFS) with a supported backup program or your backup software of choice to restore the domain database into the domain directory. See "Target Service Agents" on page 398.

   or

   On Linux or Windows, use your backup software of choice to restore the domain database into the domain directory.
3. Restart the MTA for the domain. See "Starting the MTA" on page 568.
4. To update the restored domain database with administrative changes made since it was backed up, synchronize the restored domain database with the primary domain database. See "Synchronizing a Secondary Domain" on page 365.

   If the restored domain database is for the primary domain, see "Synchronizing the Primary Domain from a Secondary Domain" on page 366.

Restoring a Post Office

Typically, damage to databases in a post office can be repaired using the database maintenance tools provided in ConsoleOne or using GroupWise Check (GWCheck). See Chapter 26, "Maintaining Domain and Post Office Databases," on page 345, Chapter 27, "Maintaining User/Resource and Message Databases," on page 353, and "GroupWise Check" on page 391.

If damage to the post office was so severe that rebuilding databases is not possible:

1. Stop the POA for the post office. See "Stopping the POA" on page 480.
2. On NetWare, use a Target Service Agent (GWTSA or TSAFS) with a supported backup program or your backup software of choice to restore the various databases into their proper locations in the post office directory. See "Target Service Agents" on page 398.

   or

   On Linux or Windows, user your backup software of choice to restore the various databases into their proper locations in the post office directory.
3. If you do not use GWTSA to restore the post office, time-stamp the restored user databases so that old items will not be automatically purged during nightly maintenance. Select the Post Office object, then click Tools > GroupWise Utilities > Backup/Restore Mailbox. On the Backup tab, select Restore, then click Yes.
4. Restart the POA for the post office. See "Starting the POA" on page 431.
5. To update the restored post office database (wphost.db) with the most current information stored in the domain database, rebuild the post office database. See "Rebuilding Domain or Post Office Databases" on page 349.
6. To update other restored databases such as user databases (user*xxx*.db) and message databases (msg*nn*.db) with the most current information stored in other post offices, run Analyze/Fix Databases with Contents selected. See "Analyzing and Fixing User and Message Databases" on page 353.

Restoring a Library

Typically, damage to library databases (dmsh.db and others) can be repaired using the database maintenance tools provided in ConsoleOne or using GroupWise Check (GWCheck). See Chapter 28, "Maintaining Library Databases and Documents," on page 359 and "GroupWise Check" on page 391.

If damage to the library is so severe that rebuilding databases is not possible:

1. Stop the POA that services the library. See "Stopping the POA" on page 480.
2. On NetWare, use a Target Service Agent (GWTSA or TSAFS) with a supported backup program or your backup software of choice to restore the library. See "Target Service Agents" on page 398.

   or

   On Linux or Windows, user your backup software of choice to restore the library.
3. Restart the POA. See "Starting the POA" on page 431.
4. To update the restored library databases with the most current information stored in other post offices, run Analyze/Fix Databases with Contents selected. Also run Analyze/Fix Library. See "Analyzing and Fixing Library and Document Information" on page 360.

Restoring an Individual Database

Typically, damage to user and resource databases (user*xxx*.db) and message databases (msg*nn*.db) can be repaired using the database maintenance tools provided in ConsoleOne or using GroupWise

Check (GWCheck). See Chapter 27, “Maintaining User/Resource and Message Databases,” on page 353 and “GroupWise Check” on page 391.

If damage to an individual database is so severe that repair is not possible:

1. Make sure the user to whom the affected database belongs is not running the GroupWise client.

2. Use your backup software of choice to restore the database into the proper location in the post office directory.

   User databases are stored in the ofuser subdirectory in the post office. Message databases are stored in the ofmsg subdirectory.

3. To update the restored database with the most current information available, run Analyze/Fix Databases with Contents selected. See “Analyzing and Fixing User and Message Databases” on page 353.

Restoring Deleted Mailbox Items

With proper planning, you can assist users in retrieving accidently deleted items and items that became unavailable because of database damage.

- “Setting Up a Restore Area” on page 381
- “Restoring a User’s Mailbox Items” on page 383
- “Letting Windows Client Users Restore Their Own Mailbox Items” on page 384

NOTE: The Cross-Platform client cannot access a restore area.

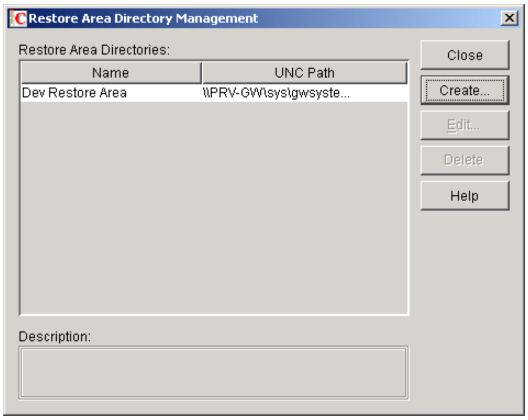
Setting Up a Restore Area

A restore area is only as useful as the post office data that is backed up regularly. Make sure you are backing up every GroupWise post office regularly, as described in “Backing Up a Post Office” on page 375.

A restore area is a location you designate to hold a backup copy of a post office so that you or GroupWise Windows client users can access it to retrieve mailbox items that are unavailable in your live GroupWise system.

To set up a restore area:

1. In ConsoleOne, click Tools > GroupWise System Operations > Restore Area Management.



Restore Area Directory Management

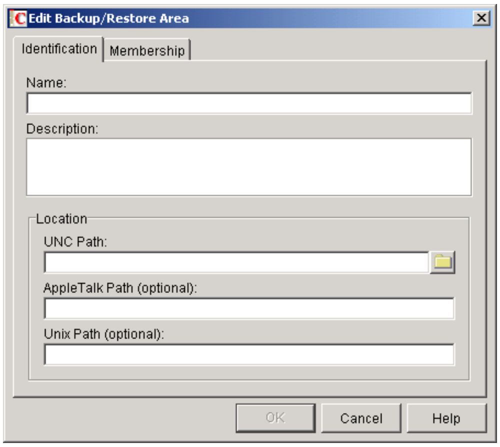
Restore Area Directories:

Name	UNC Path
Dev Restore Area	\\PRV-GW\sys\gwsyste...

Description:

The Restore Area Directory Management dialog box lists any restore areas that currently exist in your GroupWise system.

2 Click Create to set up a new restore area.



3 On the Identification tab, specify a unique name for the new restore area. If desired, provide a lengthier description to further identify the restore area.

4 In the UNC Path field, browse to and select an existing directory that you want to use as a restore area.

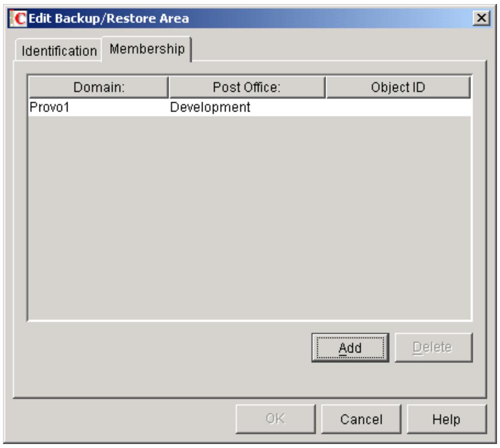
or

Specify the full path to a new directory, which will be created by the Target Service Agent that performs the restore. For more information, see "Target Service Agents" on page 398.

or

For a post office on Linux, specify the full path to an existing or new directory in the Linux Path field, so that the Linux POA can locate the restore area. The Linux POA cannot interpret a UNC path.

5 Click Membership.



Domain:	Post Office:	Object ID
Provo1	Development	

6 Click Add, select one or more post offices or users that need access to the new restore area, then click OK to add them to the membership list.

7 When the membership list is complete, click OK to create the new restore area.

If you display the Post Office Settings page for a post office that has a restore area assigned to it, you see that the Restore Area field has been filled in.

8. On NetWare, use a Target Service Agent (GWTSA or TSAFS) with a supported backup program to restore a backup copy of the post office into the restore area. See "Target Service Agents" on page 398.

   or

   Use your backup software of choice to restore the backup copy.

9. Grant the POA Read and Write rights to the restore area.

10. If the restore area is located on a different server from where the post office directory is located, provide the POA with a username and password for logging in to the remote server.

    You can provide that information using the Remote User Name and Password fields on the Post Office object's Post Office Settings page, using the /user and /password startup switches, or using the /dn startup switch.

11. If you want users to be able to retrieve individual items themselves, grant users Read and Write rights to the restore area.

12. Continue with "Restoring a User's Mailbox Items" on page 383 or "Letting Windows Client Users Restore Their Own Mailbox Items" on page 384 as needed.

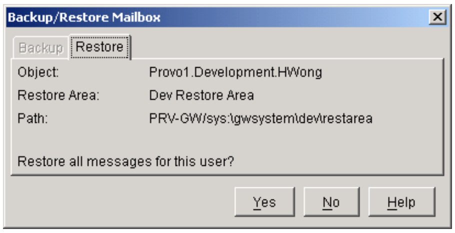
Restoring a User's Mailbox Items

After you have set up a restore area and placed a backup copy of a post office into it, you can restore a user's mailbox items for the user.

1. In ConsoleOne, browse to and select a User object for which you need to restore mailbox items.

2. Click Tools > GroupWise Utilities > Backup/Restore Mailbox.

   The Restore tab is automatically selected for you, with the restore area and directory location displayed for verification.



Object: Provo1.Development.HWong

Restore Area: Dev Restore Area

Path: PRV-GW/sys:\gwsystem\dev\restarea

Restore all messages for this user?

3. Click Yes to restore the selected user's mailbox items into his or her mailbox.

4. Notify the user and explain the following about the restored items:

   - The user might want to manually delete unwanted restored items.
   - The user should file or archive the items that he or she wants within seven days. After seven days, unaccessed items will be deleted after the amount of time allowed by existing auto-delete settings, as described in "Environment Options: Cleanup" on page 983. If auto-deletion is not enabled, the restored items will remain in the mailbox indefinitely.

Letting Windows Client Users Restore Their Own Mailbox Items

After you have set up a restore area and given Windows client users access to it, users can selectively restore individual items into their mailboxes. This saves you the work of restoring mailbox items for users and it also saves users the work of deleting unwanted restored items.

After a restore area has been set up:

1 In the GroupWise Windows client, click File > Open Backup.

2 Browse to and select the restore area directory, then click OK.

3 In the Password field, type your GroupWise password, then click OK to access the backup copy of your mailbox.

4 Retrieve individual items as needed.

The backup copy of your mailbox offers basic features such as Read, Search, and Undelete so that you can locate and retrieve the items you need.

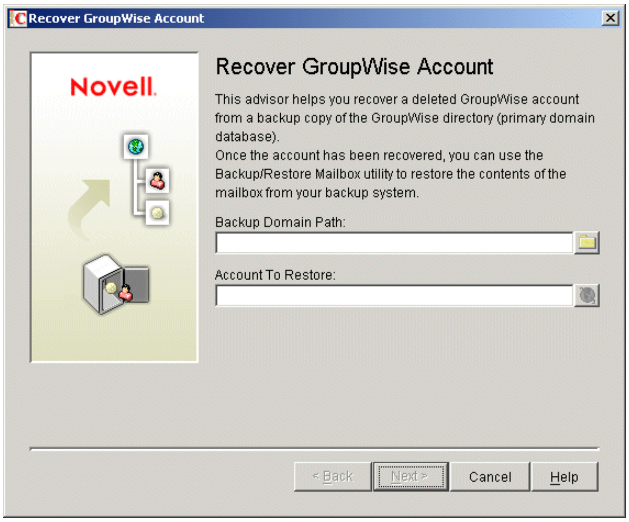
5 When you are finished restoring items to your live mailbox, click File > Open Backup again to remove the check mark from the Open Backup option and return to your live mailbox.

Recovering Deleted GroupWise Accounts

If you have a reliable backup procedure in place, as described in Chapter 31, "Backing Up GroupWise Databases," on page 375, you can restore recently deleted GroupWise user and resource accounts.

1 Make available a backup copy of a domain database (wpdomain.db) where the deleted GroupWise account still exists.

2 In ConsoleOne, click Tools > GroupWise Utilities > Recover Deleted Account.

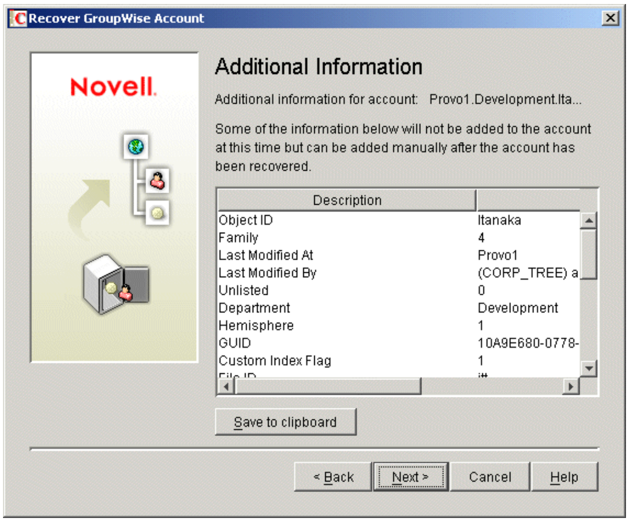


This advisor helps you recover a deleted GroupWise account from a backup copy of the GroupWise directory (primary domain database).
Once the account has been recovered, you can use the Backup/Restore Mailbox utility to restore the contents of the mailbox from your backup system.

3 Browse to and select the backup copy of the domain database.

4 Select the user or resource that you need to recover the account for.

5 Click Next.



Additional Information

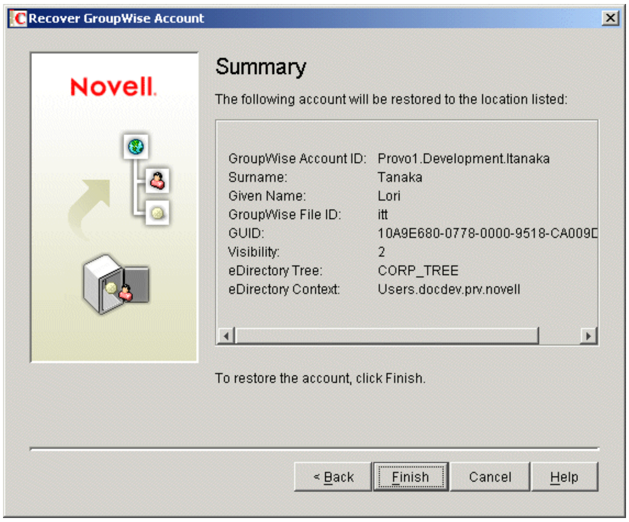
Additional information for account: Provo1.Development.lta...

Some of the information below will not be added to the account at this time but can be added manually after the account has been recovered.

Description	
Object ID	ltanaka
Family	4
Last Modified At	Provo1
Last Modified By	(CORP_TREE) a
Unlisted	0
Department	Development
Hemisphere	1
GUID	10A9E680-0778-
Custom Index Flag	1
File ID	itt

6 If desired, click Save to Clipboard, paste it into a file, then save or print it.

7 Click Next.



Summary

The following account will be restored to the location listed:

GroupWise Account ID:	Provo1.Development.ltanaka
Surname:	Tanaka
Given Name:	Lori
GroupWise File ID:	itt
GUID:	10A9E680-0778-0000-9518-CA009D
Visibility:	2
eDirectory Tree:	CORP_TREE
eDirectory Context:	Users.docdev.prv.novell

To restore the account, click Finish.

8 Click Finish.

At this point, you have restored the user’s or resource’s GroupWise account into the GroupWise system. However, this does not restore ownership of resources, nor does the account’s mailbox contain any item at this point.

9 If the restored user owned resources, manually restore the ownership. See “Changing a Resource’s Owner” on page 227

10 To restore the contents of the account’s mailbox, follow the instructions in “Restoring Deleted Mailbox Items” on page 381.

33 Retaining User Messages

GroupWise® enables you to retain user messages until they have been copied from message databases to another storage location. This means that a user cannot perform any action, such as emptying the mailbox Trash, that will result in a message being removed from the message database before it has been copied.

Message retention primarily consists of two activities: 1) not allowing users to remove messages until they have been retained and 2) retaining the messages by copying them from message databases to another location.

GroupWise supplies the ability to not allow users to remove messages until they've been retained. It also provides methods for message retention applications to securely access user mailboxes and copy messages. However, it does not provide the message retention application. You must develop or purchase a third-party (non-GroupWise) application that performs this service.

- "How Message Retention Works" on page 387
- "Acquiring a Message Retention Application" on page 389
- "Enabling Message Retention" on page 389

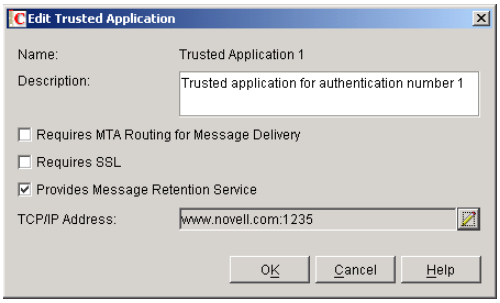
How Message Retention Works

To understand how message retention works, you need to understand what GroupWise does and what the message retention application does, as explained in the following sections:

- "What GroupWise Does" on page 387
- "What the Message Retention Application Does" on page 388

What GroupWise Does

During installation of the message retention application, the application uses the GroupWise Trusted Application API to create a trusted application record in the GroupWise system. The trusted application record includes a flag that designates it as a message retention application. This flag is surfaced through the trusted application's Provides Message Retention Service setting in ConsoleOne (Tools menu > GroupWise System Operations > Trusted Applications > Edit).



Name: Trusted Application 1

Description: Trusted application for authentication number 1

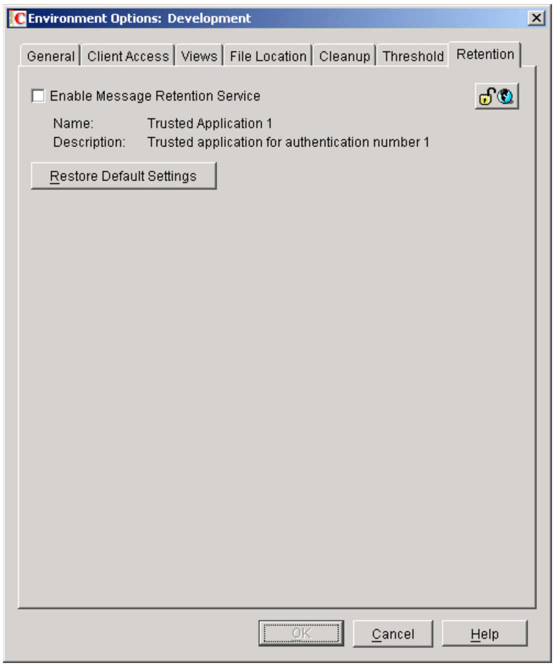
☐ Requires MTA Routing for Message Delivery

☐ Requires SSL

☑ Provides Message Retention Service

TCP/IP Address: www.novell.com:1235

When ConsoleOne reads a trusted application record that has the Provides Message Retention Service setting turned on, it adds a Retention tab to the GroupWise Client Environment Options (Tools menu > GroupWise Utilities > Client Options > Environment).



□ Enable Message Retention Service

Name: Trusted Application 1

Description: Trusted application for authentication number 1

You use this Retention tab to enable message retention at the domain, post office, or user level, meaning that you can enable it for all users in a domain, all users in a post office, or individual users.

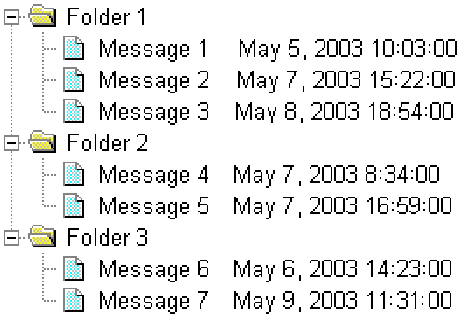
Turning on message retention alters the GroupWise client purge behavior by preventing a user from purging any messages from his or her mailbox that have not yet been retained.

What the Message Retention Application Does

Different message retention applications might vary slightly in their approach to retaining messages. This section provides a general approach to message retention.

To determine whether or not mailbox messages have been retained, the message retention application adds a time stamp to the mailbox. The message retention application can use the GroupWise Object API or GroupWise IMAP support to write (and read) the time stamp. In addition, you can use the GroupWise Time Stamp Utility (page 405) to manually set the time stamp.

The time stamp represents the most recent date and time that message retention was completed for the mailbox. Messages delivered after the time stamp cannot be purged until they have been retained. This requires that the message retention application retain items chronologically, oldest to newest. For example, assume a mailbox has a message retention time stamp of May 7, 2003 12:00:00. The mailbox has three folders with a total of seven messages:



```
Folder 1
    Message 1    May 5, 2003 10:03:00
    Message 2    May 7, 2003 15:22:00
    Message 3    May 8, 2003 18:54:00
Folder 2
    Message 4    May 7, 2003 8:34:00
    Message 5    May 7, 2003 16:59:00
Folder 3
    Message 6    May 6, 2003 14:23:00
    Message 7    May 9, 2003 11:31:00
```

The message retention application reads the existing time stamp (May 7, 2003 12:00:00) and selects a time between that time and the current time. For example, suppose the current time is May 9, 2003 14:00:00. The message retention application could choose May 8, 2003 12:00:00 as the new time stamp. It would then retain any messages delivered between the existing time stamp (May 7, 2003 12:00:00) and the new time stamp (May 8, 2003, 12:00:00).

In the above example, messages 1, 4, and 6 are older than the existing time stamp (May 7, 2003 12:00:00). The message retention application would not retain these messages again, assuming that they had already been safely retained. Messages 2 and 5 have dates that fall between the existing time stamp (May 7, 2003 12:00:00) and the new time stamp (May 8, 2003, 12:00:00) so they would be retained. Messages 3 and 7 have dates that fall after the new time stamp (May 8, 2003, 12:00:00) so they would not be retained until the next time the message retention application ran against the mailbox.

Acquiring a Message Retention Application

If you do not already have a message retention application to use with GroupWise, you have two options: 1) you can purchase an application from a GroupWise partner or 2) you can develop your own application.

For information about GroupWise partners that provide message (e-mail) retention applications, see the Partner Product Guide (http://www.novell.com/partnerguide/).

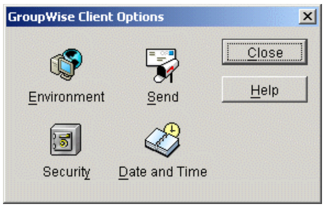
For information about developing a message retention application, see the *GroupWise Object API* and *GroupWise Trusted Application API* documentation at the Novell Developer Kit Web site (http://developer.novell.com/ndk).

Enabling Message Retention

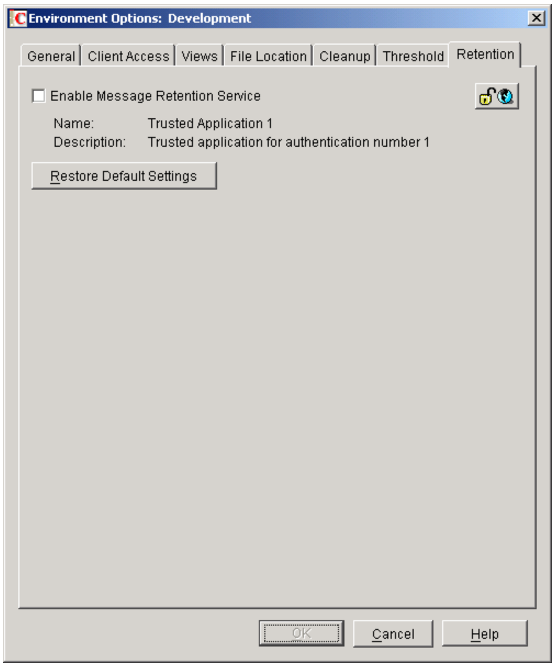
This section assumes that you've installed a message retention application as a GroupWise trusted application and that it is configured to provide a message retention service. If not, see "Trusted Applications" on page 62.

Message retention is not enabled until you designate the users whose messages you want retained by the application. You can designate users at the domain level, post office level, or individual user level.

1. In ConsoleOne, right-click the domain, post office, or user for which you want to enable message retention, click GroupWise Utilities > Client Options to display the GroupWise Client Options dialog box.



2 Click Environment to display the Environment Options dialog box, then click the Retention tab.



□ Enable Message Retention Service

Name: Trusted Application 1

Description: Trusted application for authentication number 1

3 Turn on the Enable Message Retention Service setting.

4 If you want to lock the setting at this level, click the Lock button.

For example, if you lock the setting at the domain level, the setting cannot be changed for any post offices or users within the domain. If you lock the setting at the post office level, it cannot be changed individually for the post office's users.

This setting does not display in the GroupWise client. Therefore, there is no lock available when editing this setting for individual users.

5 Click OK to save the changes.

34 Standalone Database Maintenance Programs

Some aspects of GroupWise® database maintenance are performed by standalone maintenance programs that can be incorporated into batch files along with other system maintenance programs.

- "GroupWise Check" on page 391
- "Target Service Agents" on page 398
- "GroupWise Time Stamp Utility" on page 405
- "GroupWise Database Copy Utility" on page 412

GroupWise Check

GroupWise Check (GWCheck) is a tool provided for GroupWise that will check and repair GroupWise user, message, library, and resource databases without needing ConsoleOne®. In addition to checking post office, user, and library databases, it will also check users' remote, caching, and archive databases.

- "GWCheck Functionality" on page 391
- "Starting GWCheck on a Windows Workstation" on page 393
- "Starting GWCheck on a Linux Workstation" on page 394
- "Using GWCheck on a Workstation" on page 395
- "Executing GWCheck from a Windows Batch File" on page 398
- "Executing GWCheck from a Linux Script" on page 398
- "GroupWise Check Error Codes"

NOTE: GWCheck is not currently available for use on Macintosh workstations.

GWCheck Functionality

The GWCheck utility begins by comparing three databases.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
The post office database (wphost.db) is checked for the file ID (FID) of the selected user.	The guardian database (ngwguard.db) is checked to find out if this user database has been created.	The file system for this post office is checked to see if the user database (user*xxx*.db) for this user exists.

After GWCheck makes the database comparisons, it begins processing according to the databases selected and any inconsistencies found.

Case 1 - Missing Entry in the Post Office Database (wphost.db)

In this example, a contents check is run either against all users on the post office or against one user, "ABC." GWCheck does not find the FID of one or more users.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
?	userabc.db	userabc.db
No entry for this user is found in the post office database (wphost.db).	An entry is found in the guardian database (ngwguard.db), indicating that the user has been deleted.	Also, a user database (user*xxx*.db) for this user is found in the ofuser directory.

GWCheck will remove the entry from ngwguard.db, delete userabc.db and systematically delete all of the user's messages from the message databases that are not still being referenced by other users. If the user has been deleted, GWCheck will clean up after that user.

WARNING: If a post office database becomes damaged so some users are unable to log in, GWCheck should not be run until the post office has been rebuilt. For more information, see "Rebuilding Domain or Post Office Databases" on page 349.

Case 2 - Missing Entry in the Guardian Database (ngwguard.db)

In this example, a GWCheck is run either against all users on the post office or against one user, "ABC." A user's FID is found and the user's database is found in the post office, but the user is missing in ngwguard.db.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
FID abc	?	userabc.db
The user appears in the post office database (wphost.db).	The guardian database (ngwguard.db) shows no user database for this user.	A user database (user*xxx*.db) for the user does exist in the ofuser directory.

GWCheck will create the user in ngwguard.db, using database userabc.db. Even if ngwguard.db is damaged, it is unlikely that data will be lost.

Case 3 - Missing User Database (user*xxx*.db)

In this example, a GWCheck is run either against all users on the post office or against one user, "ABC." The user's FID is found, as well as the user's record in ngwguard.db. However, the user's database is not found.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
FID abc	userabc.db	?
The user is found in the post office database (wphost.db).	The user is found in the guardian database (ngwguard.db).	No user database (user*xxx*.db) is found in the ofuser directory.

GWCheck will take actions depending on what options are selected.

Contents Check: GWCheck will delete all of this user's messages from the message databases if they are not referenced by other users.

Structural Rebuild: GWCheck will create a blank user database for this user. Existing messages for this user will be ignored.

Re-create User Database: GWCheck will create a blank user database for this user and populate it with messages in the message databases that have been sent to or from this user.

WARNING: If a user database has been deleted, do not run a Contents Check until after a Structural Rebuild or Re-create User Database has been run for that user. For more information, see "Performing a Structural Rebuild of a User Database" on page 355 and "Re-creating a User Database" on page 356.

Starting GWCheck on a Windows Workstation

You can use GWCheck on any Windows 98/NT/2000/XP workstation.

As an administrator, you can run GWCheck for databases in any post office accessible from the workstation where GWCheck is installed. The GWCheck program performs all database maintenance itself, rather than handing off a task to the POA as ConsoleOne would do to perform database maintenance.

Depending on how GroupWise Check is installed, users might have a Repair Mailbox item on the GroupWise Windows client Tools menu that enables them to run GWCheck from the client. If the GWCheck program is available to users, users can perform database maintenance on their Remote, Caching, and archive mailboxes, which are not accessible from ConsoleOne.

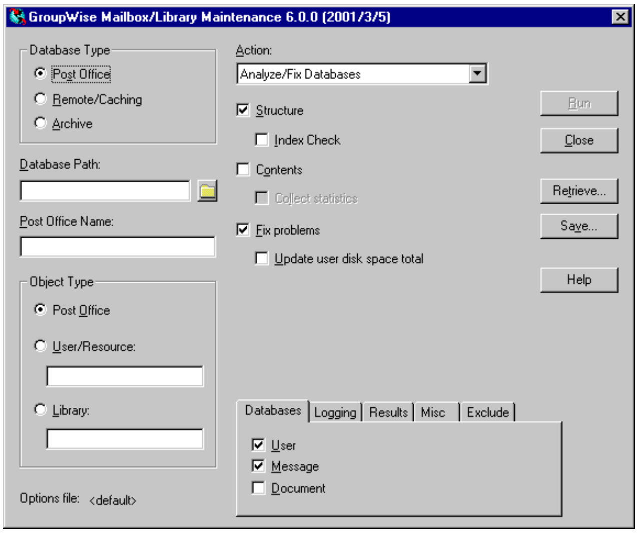
For the Repair Mailbox item to display on the GroupWise Windows client Tools menu, the following files must be installed in the GroupWise directory; by default, this is c:\novell\groupwise.

- gwcheck.exe
- gwchk*xx*.dll (Replace *xx* with your language code)
- gwchk*xx*.chm (Replace *xx* with your language code)

The GroupWise administrator can install these files by using SetupIP to install the GroupWise Windows client, and selecting to install and enable GWCheck. The default for SetupIP is to install GWCheck, but not enable GWCheck. The files are then copied to the \novell\groupwise\gwcheck directory. For additional information about SetupIP and GWCheck, see "[GWCHECK]" on page 1009.

If the client was installed from the installation program on the CD or the defaults are chosen for SetupIP, the client user needs to copy the files from the GWCheck directory (\novell\groupwise\gwcheck) to the main GroupWise directory (\novell\groupwise\).

1 From the Start menu, click Run, then browse to and double-click gwcheck.exe.



GroupWise Mailbox/Library Maintenance 6.0.0 (2001/3/5)

Database Type
● Post Office
○ Remote/Caching
○ Archive

Database Path:

Post Office Name:

Object Type
● Post Office
○ User/Resource:
○ Library:

Options file: <default>

Action: Analyze/Fix Databases

☑ Structure
☐ Index Check
☐ Contents
☐ Collect statistics
☑ Fix problems
☐ Update user disk space total

Databases
☑ User
☑ Message
☐ Document

2 To view online help in GWCheck, click Help.

3 Continue with "Using GWCheck on a Workstation" on page 395.

Starting GWCheck on a Linux Workstation

You can use GWCheck on any Linux workstation where you can run the Cross-Platform client. GWCheck is not installed along with the client, so you must install it manually.

1 Change to the directory where the GWCheck RPM is located or copy it to a convenient location on your workstation.

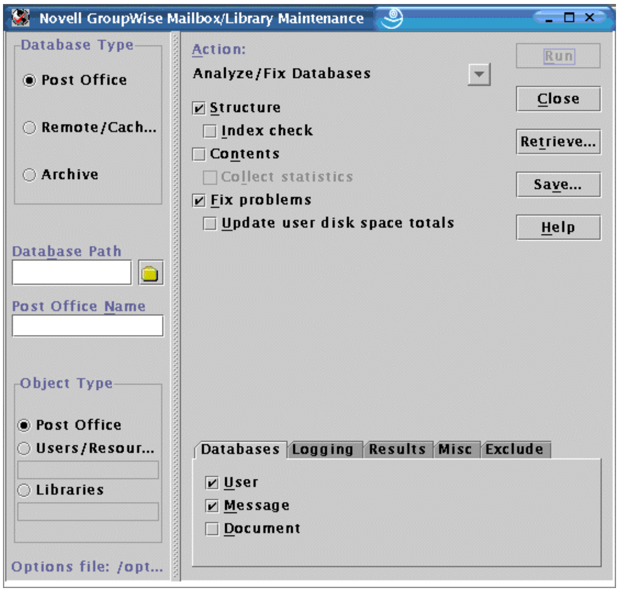
The GWCheck RPM (groupwise-gwcheck-6.5.1-*mmdd*.i386.rpm) is located in the /client and /admin directories in your GroupWise software distribution directory if it is has been updated or on the *GroupWise 6.5 for Linux Administrator* CD if an updated software distribution directory is not available.

2 Install GWCheck.

```
rpm -i groupwise-gwcheck-6.5.1-mmdd.i386.rpm
```

3 Change to the /opt/novell/groupwise/gwcheck/bin directory.

4 Enter `./gwcheck` to start GWCheck.



Database Type

● Post Office

○ Remote/Cach...

○ Archive

Database Path

Post Office Name

Object Type

● Post Office

○ Users/Resour...

○ Libraries

Options file: /opt...

Action:

Analyze/Fix Databases

☑ Structure

□ Index check

□ Contents

□ Collect statistics

☑ Fix problems

□ Update user disk space totals

☑ User

☑ Message

□ Document

5 To view online help in GWCheck, click Help.

6 Continue with Using GWCheck on a Workstation.

Using GWCheck on a Workstation

With only a few differences in interface functionality, as described in the online help, you can perform the same maintenance activities in GroupWise Check as you can in Mailbox/Library Maintenance in ConsoleOne:

- "Analyzing and Fixing User and Message Databases" on page 353
- "Performing a Structural Rebuild of a User Database" on page 355
- "Re-creating a User Database" on page 356
- "Analyzing and Fixing Databases for Libraries and Documents" on page 359
- "Analyzing and Fixing Library and Document Information" on page 360
- "Gathering Mailbox Statistics" on page 367
- "Reducing the Size of User and Message Databases" on page 369
- "Reclaiming Disk Space in Domain and Post Office Databases" on page 370
- "Archiving and Deleting Documents" on page 372
- "Deleting Activity Logs" on page 373
- "Using Mailbox/Library Maintenance Tab Options" on page 395
- "Reusing Library/Mailbox Maintenance Settings" on page 397

Using Mailbox/Library Maintenance Tab Options

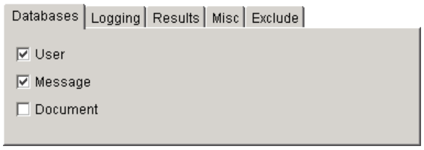
Both GroupWise Check and Mailbox/Library Maintenance in ConsoleOne use tab options to control the checking process.

- "Databases" on page 396
- "Logging" on page 396

- “Results” on page 396
- “Misc” on page 397
- “Exclude” on page 397

Databases

To select the types of database to perform the Mailbox/Library Maintenance check on, click Databases.



☑ User
☑ Message
□ Document

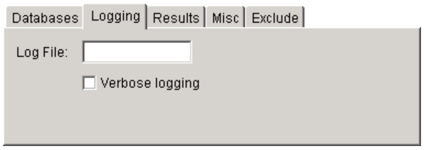
Depending on the object type and action already selected in the main window, some database types might be unavailable. If all the database types are unavailable, then one or more database types have been pre-selected for you.

You can perform an action on the following databases when the type is not unavailable:

- **User:** Checks the user databases.
- **Message Databases:** Checks the message databases.
- **Document:** Checks the library and document properties databases.

Logging

To specify the name of the file where you want the results of the MailBox/Library Maintenance check to be stored, click Logging.



Log File:
□ Verbose logging

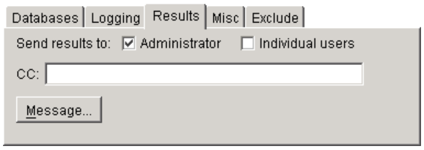
Specify a file name. By default, the file is created in the *post_office_directory*\wpcsout\ofs directory. To redirect the log file to another location, specify a full path and file name. Use a UNC path, or make sure the mapped drive path is from the perspective of the POA.

Click Verbose Logging to log detailed information. Verbose logging might produce large log files and slow execution.

This file will be sent to the users selected on the Results tab.

Results

To select users to receive the results of the Mailbox/Library Maintenance check, click Results.

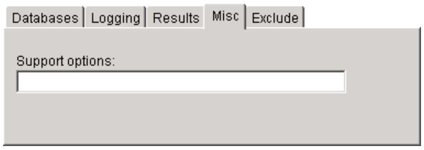


Send results to: ☑ Administrator □ Individual users
CC:

Select Administrator to send the results to the user defined as the GroupWise domain administrator. Select Individual Users to send each user the results that pertain to him or her. Click Message to include a message with the results file.

Misc

If you need to run a Mailbox/Library Maintenance check with special options provided by Novell Support, click Misc.

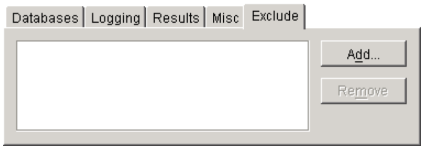


Support options:

Use the Support Options field to specify command line parameters. Support options are typically obtained from Novell Support representatives when you need assistance resolving specific database problems. Search the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp) for TIDs and Support Pack Readmes that list support options. Make sure that you clearly understand what the Support options do before you use them.

Exclude

If you want to exclude certain users in the selected post office from having the Mailbox/Library Maintenance check performed on their databases, click Exclude.



Click Add, select one or more users to exclude, then click OK.

Reusing Library/Mailbox Maintenance Settings

For convenience, you can store the options you select in Mailbox/Library Maintenance and GroupWise Check so that you can retrieve them for later use.

- "Saving Mailbox/Library Maintenance Options" on page 397
- "Retrieving Mailbox/Library Maintenance Options" on page 397

Saving Mailbox/Library Maintenance Options

1 After you have selected all of the options in the Mailbox/Library Maintenance dialog box, click Save.

2 Browse to the directory where you want to save the options file if you do not want to use the default of wptools in the domain to which you're currently connected.

3 Enter a file name if you do not want to use the default of gwcheck.opt.

4 Click Save.

Retrieving Mailbox/Library Maintenance Options

1 In the Mailbox/Library Maintenance dialog box, click Retrieve.

2. Browse to and select your saved option file.
3. Click Open.

Executing GWCheck from a Windows Batch File

The GWCheck program is located in the \admin\utilities\gwcheck directory in your GroupWise software distribution directory if it has been updated or on the *GroupWise 6.5 Administrator* CD if an updated software distribution directory is not available. It might also be installed along with the GroupWise client software in the gwcheck subdirectory of the client installation directory.

1. Use the following syntax to create a batch file to execute GWCheck:

   ```
   gwcheck /opt=options_file /batch
   ```

   If you want to include the path to an archive database, use the /pa switch.
2. To create an options file, see "Saving Mailbox/Library Maintenance Options" on page 397.

Executing GWCheck from a Linux Script

The GWCheck program is located in the /admin directory in your GroupWise software distribution directory if it has been updated or on the *GroupWise 6.5 for Linux Administrator* CD if an updated software distribution directory is not available.

1. Make sure that GWCheck has been installed, as described in "Starting GWCheck on a Linux Workstation" on page 394
2. Create a script to execute GWCheck using the following syntax:

   ```
   /opt/novell/groupwise/gwcheck/bin --opt options_file --batch
   ```

   If you want to include the path to an archive database, use the --pa switch.
3. To create an options file, see "Saving Mailbox/Library Maintenance Options" on page 397.

Target Service Agents

A Target Service Agent (TSA) helps generic backup software back up specialized data located on any "target." A target is a specific location where data is stored, such as a NetWare file system, an eDirectory database, or a collection of GroupWise databases. A target could also be an application that provides data to be backed up. A TSA is specialized to scan, read, and write the specific types of data available at the target. A TSA serves as an intermediary between specific data types and a general backup engine.

The GroupWise Target Service Agent (GWTSA) has long been included with GroupWise and can back up GroupWise data stored on NetWare 4.2, 5.1, and 6.*x* servers. It is specialized to back up specific GroupWise data types, such as domains and post offices.

The NetWare Target Service Agent for File Systems (TSAFS), available on NetWare 6.*x* (but not on earlier versions of NetWare), includes a startup option enabling it to handle GroupWise data. TSAFS includes file system backup enhancements that GWTSA does not provide.

For optimum backups on NetWare, select the Target Service Agent appropriate for your version of NetWare and GroupWise:

- "GroupWise Target Service Agent" on page 399
- "NetWare Target Service Agent for File Systems" on page 403

GroupWise Target Service Agent

The GroupWise Target Service Agent (GWTSA) provides reliable backups of a running GroupWise system on NetWare by successfully backing up open files and locked files, rather than skipping them.

- "GWTSA Functionality" on page 399
- "Running GWTSA" on page 400
- "GWTSA Startup Switches" on page 403

GWTSA Functionality

The GroupWise Target Service Agent (GWTSA) works with other backup software on NetWare. For a complete and current list of compatible backup software, use the Partner Product Guide (http://www.novell.com/partnerguide).

GWTSA has no user interface of its own, but its presence running along with other backup software provides GroupWise options in the backup software that would not otherwise be available. As a Target Service Agent, GWTSA supports any feature that your backup software supports. So if your backup software supports full, incremental, and differential backups or working set and copy jobs, so does GWTSA.

GWTSA backs up standard GroupWise directories and files; extra directories and files that appear within a standard GroupWise directory structure are not backed up by GWTSA. The table below lists the directories and files that are backed up by GWTSA.

GroupWise Location	Directories	Subdirectories/Files Backed Up
Domain	*domain_directory*	wpdomain.db wpdomain.dc wphost.dc gwdom.dc gwpo.dc mtaname
	domain_directory\wpgate	async gwia webac60a etc.

GroupWise Location	Directories	Subdirectories/Files Backed Up
Post Office	*post_office_directory*	wphost.db ngwguard.db ngwguard.dc ngwguard.rfl ngwguard.fbk ngwcheck.db ngwcheck.log gwpo.dc
	post_office_directory\gwdms	dmsh.db
	post_office_directory\gwdms\library_directory	*.db archive\*.* docs\*.*
	post_office_directory\offiles	*.*
	post_office_directory\ofmsg	*.*
	post_office_directory\ofmsg\guardbak	ngwguard.fbk
	post_office_directory\ofuser	user*xxx*.db
	post_office_directory\ofuser\index	*.idx *.inc
	post_office_directory\ofviews\win	*.vew *.ini
Library (Document Storage Area)	*library_directory*	*.db archive\*.* docs\*.*

To see directory structure diagrams showing where the files are located, see "Domain Directory" and "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

GWTSA automatically time-stamps all backed-up user databases (user*xxx*.db), so that the Allow Purge of Items Not Backed Up option described in "Modifying Environment Options" on page 977 can function to safeguard users' deleted items against being purged from your GroupWise system before they have been backed up.

IMPORTANT: If you decide not to use GWTSA, user databases must be time-stamped as a separate process in order for the purge control environment option to work properly. For instructions, see "GroupWise Time Stamp Utility" on page 405.

Running GWTSA

GWTSA is available for use on NetWare 4.2, 5.1, and 6.*x*. The gwtsa.nlm program file is automatically installed along with the GroupWise agents (POA and MTA). If the domains and post offices to back up are located on a different server from where the agents run, you must copy GWTSA (gwtsa.nlm), along with the agent engine (gwenn4.nlm), to the server where the data resides and run it there.

During agent installation, a gwtsa.ncf file is created in the directory where you installed the agents. By default, it loads gwtsa.nlm and provides a /home switch for each domain and post office you selected to be serviced by the MTA and POA. For example:

Syntax:

```
load sys:\system\gwtsa /home-domain_directory
                       /home-post_office_directory
```

Example:

```
load sys:\system\gwtsa /home-sys:\gwsystem\provo1
                       /home-sys:\gwsystem\dev
```

You can add additional instances of the /home switch to back up more domains and post offices.

Syntax:

```
load sys:\system\gwtsa /home-domain_directory
                       /home-domain_directory
                       /home-post_office_directory
                       /home-post_office_directory
                       /home-post_office_directory
```

Example:

```
load sys:\system\gwtsa /home-sys:\gwsystem\provo1
                       /home-sys:\gwsystem\provo2
                       /home-sys:\gwsystem\dev
                       /home-sys:\gwsystem\sales
                       /home-sys:\gwsystem\research
```

You can also add instances of the /home switch to point to restore areas for post offices or to other temporary locations where you want to restore data.

By default, GWTSA places temporary files in the sys:\system\temp directory during the backup process. If necessary, use the /tempdir switch to specify an alternate location where more disk space is available for temporary files. Additional configuration of GWTSA can be done using other startup switches. See "GWTSA Startup Switches" on page 403 for a complete list.

To start GWTSA immediately, run the gwtsa.ncf file at the NetWare server console. To start GWTSA automatically each time you restart the server, add a gwtsa.ncf line to the autoexec.ncf file. With GWTSA running, you are ready to back up GroupWise data with Novell Storage Management Services or other compatible backup software.

Using GWTSA with Your Backup Software

The GWTSA adds GroupWise options to your backup software. This section uses Novell Storage Management Services (SMS) and the NetWare Backup utility (nwback32.exe) as an example of how to integrate GWTSA into your backup software. Similar steps are necessary to integrate GWTSA with other backup software.

If you plan to use GWTSA with SMS, this section assumes that SMS has been installed and configured and is running properly. If you need assistance with SMS, refer to *Backup and Restore Services (Storage Management Services)* on the NetWare 6.5 Documentation Web site (http://www.novell.com/documentation/nw65/index.html).

- "Backing Up GroupWise Data with SMS" on page 402
- "Restoring GroupWise Data with SMS" on page 402

NOTE: If you are using Veritas Backup Exec 9 for NetWare, be sure to deselect Delete Existing Trustees on the Backup Exec NetWare tab when you are creating a restore job. If you do not deselect Delete Existing Trustees, GWTSA cannot restore any file that has a .db extension. All GroupWise databases have a .db extension.

Backing Up GroupWise Data with SMS

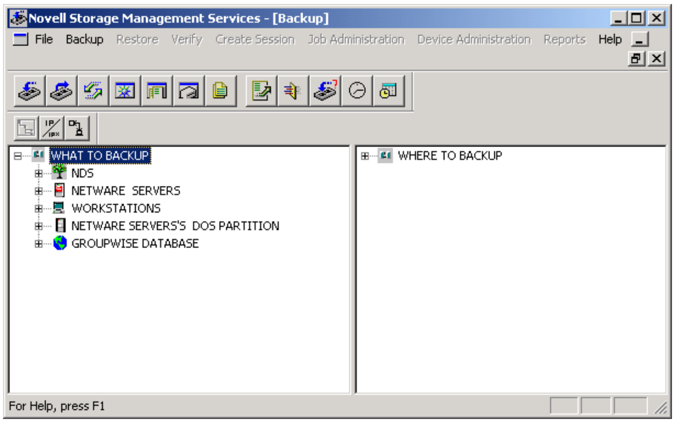
To back up GroupWise data using SMS with GWTSA running:

1. Start nwback32.exe from the sys:\public directory of your NetWare server.

   You can also use sbcon.nlm at the NetWare server console to perform the backup.

2. In the Quick Access dialog box, click Backup.

3. Expand the WHAT TO BACKUP object.



   A GROUPWISE DATABASE object has been added to the list of things you can back up.

4. Expand the GROUPWISE DATABASE object to list GroupWise domains, post offices, and libraries that are available for backup.

5. After selecting the GroupWise data to back up, continue using SMS as you usually would to perform the backup.

Restoring GroupWise Data with SMS

To restore GroupWise data using SMS with GWTSA running:

1. Start nwback32.exe from the sys:\public directory of your NetWare server.

   You can also use sbcon.nlm at the NetWare server console to restore GroupWise data.

2. In the Quick Access dialog box, click Restore.

3. Expand the WHAT TO RESTORE object, then select your backup device.

4. Expand the WHERE TO RESTORE object.

   A GROUPWISE DATABASE object appears on the list of things you can restore.

5. Expand the GROUPWISE DATABASE object to list GroupWise domains, post offices, libraries, and restore areas where data can be restored.

6. After selecting the GroupWise data to restore, continue using SMS as you usually would to restore data.

If you need to restore GroupWise data to an existing domain, post office, or library, make sure your backup software is configured to overwrite *newer* files than those that are being restored.

If you are restoring GroupWise data to a temporary location, make sure you have sufficient free disk space to accommodate the files that are being restored.

GWTSA Startup Switches

The following startup switches can be used with GWTSA:

/home
Specifies the GroupWise location to back up or restore to. Multiple instances of the /home switch are typical. Use a /home switch for each domain and post office to back up. Also use a /home switch for each post office restore area and any other temporary location to which you want to restore GroupWise data outside the standard GroupWise directory structure.

/tempdir
Specifies where GWTSA places its temporary files during the backup process. The default is the sys:\system\tsa\temp directory.

/log
Turns on logging and displays a logging screen. By default, logging is turned off. When you turn logging on, a gwtsa.log file is created in the sys:\system\tsa directory.

/ll
Sets the log level to determine how much information is written to GWTSA log file. Use `n` for Normal and `v` for Verbose.

NetWare Target Service Agent for File Systems

The Target Service Agent for File Systems (TSAFS) is available on NetWare 6.0 and later.

- "TSAFS Functionality" on page 403
- "Running TSAFS" on page 404
- "Using TSAFS with Novell Storage Management Service (SMS)" on page 404

IMPORTANT: If you are using GroupWise 6.5 Support Pack 3 or later, TSAFS can time-stamp GroupWise databases as part of the backup process. If you are using an earlier version of GroupWise, time stamping must be performed as a separate process, as described in "GroupWise Time Stamp Utility" on page 405.

TSAFS Functionality

The Target Service Agent for File Systems (TSAFS) includes enhancements that earlier versions of TSAFS did not include:

- Supports GroupWise database lock/backup/unlock functionality so that you can back up a running GroupWise system
- Provides time stamping of GroupWise 6.5.3 and later user databases so that the Allow Purge of Items Not Backed Up option described in "Modifying Environment Options" on page 977 can function to safeguard users' deleted items against being purged from your GroupWise system before they have been backed up
- Supports backups of clustered servers so that the backup job continues on failover
- Uses a read-ahead, data caching mechanism to improve backup performance

For complete details about the TSAFS, see the *NetWare 6.5 Storage Management Services Administration Guide* on the NetWare 6.5 Documentation page (http://www.novell.com/documentation/nw65/index.html).

Running TSAFS

At your NetWare server console, unload TSAFS, then use the following command to start TSAFS with GroupWise functionality:

```
load tsafs /EnableGW=True
```

The switch setting is saved in a configuration file, so that you do not need to include the switch when you load tsafs.nlm in the future.

To start TSAFS automatically each time you restart the server, load tsafs.nlm in the autoexec.ncf file.

To run TSAFS without GroupWise functionality, unload TSAFS, then reload using:

```
load tsafs /EnableGW=False
```

To determine whether or not TSAFS is running with GroupWise functionality, use:

```
tsafs
```

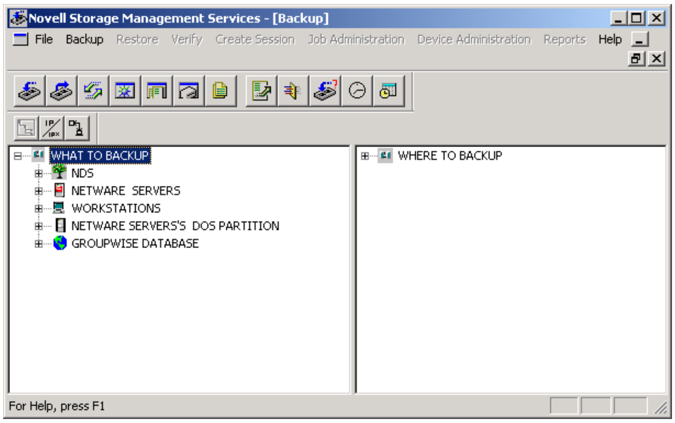
Scroll down to the /EnableGW entry and look for a value of True or False.

Using TSAFS with Novell Storage Management Service (SMS)

1 After TSASF is running on the NetWare server, start the NetWare Backup utility (nwbackup32.exe) on a Windows machine.

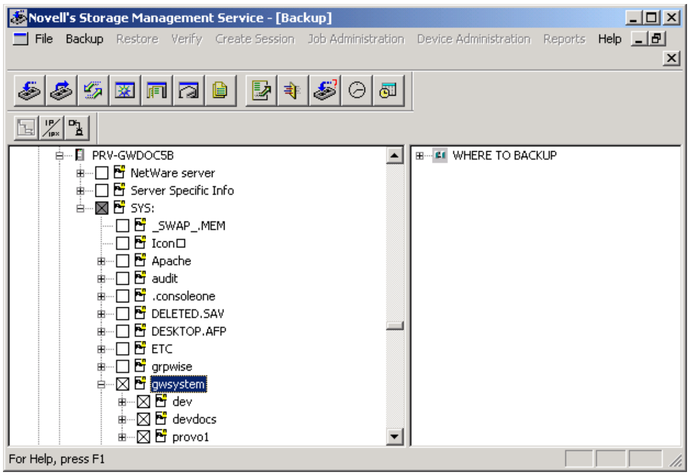
   You can also use sbcon.nlm at the NetWare server console to perform the backup.

2 In the Quick Access dialog box, click Backup, then expand WHAT TO BACKUP.



   The GROUPWISE DATABASES item is listed if you have been using the GroupWise Target Service Agent (GWTSA). Do not use it with TSAFS.

3 Expand NETWARE SERVERS, then browse to and select directories where GroupWise domains, post offices, and document storage areas are located.



For background information about GroupWise directory structures, see "Domain Directory" and "Post Office Directory" in "Directory Structure Diagrams" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

4 Configure the backup job as needed, as described in *NetWare 6.5 Storage Management Services Administration Guide* on the NetWare 6.5 Documentation page (http://www.novell.com/documentation/nw65/index.html).

To avoid error messages caused by open files that do not need to be backed up, some files can be excluded from the backup, for example:

- Agent log files (*mmdd*poa.*nnn*, *mmdd*mta.*nnn*, *mmdd*gwia.*nnn*, and *mmdd*web.*nnn*)
- Internet Agent lock and cycle files (proc and pulse.tmp)
- Transitory xNStore files used briefly by the agents in the message queues

5 When you have finished configuring the backup job, click Backup > Submit the Job.

If you need to restore GroupWise data, be sure to run GroupWise Check (GWCheck) as described in Chapter 32, "Restoring GroupWise Databases from Backup," on page 379.

GroupWise Time Stamp Utility

You can use the GroupWise Time Stamp (GWTMSTMP) utility to ensure that GroupWise user databases include the dates when they were last backed up, restored, and retained.

The following sections provide information about the utility:

- "GWTMSTMP Functionality" on page 406
- "Running GWTMSTMP on NetWare" on page 406
- "Running GWTMSTMP on Linux" on page 407
- "Running GWTMSTMP on Windows" on page 407
- "GWTMSTMP Startup Switches" on page 408

NOTE: GWTMSTMP is available in GroupWise 6.5 for Linux Support Pack 2, but not in the original release of GroupWise 6.5 for Linux. Time stamp functionality is included in the NetWare Target Service Agent for File Systems (TSAFS) for GroupWise 6.5 systems where Support Pack 3 has been installed, so you do not need to use GWTMSTMP when backing up a GroupWise 6.5.3 system with TSAFS.

GWTMSTMP Functionality

GWTMSTMP places date and time information on user databases (user*xxx*.db) in order to support message backup, restore, and retention. No other databases are affected. You can run GWTMSTMP on all user databases in a post office or on a single user database.

Backup

To ensure thorough user database backups, you can make sure that deleted items are not purged from users' databases until they have been backed up. Two conditions must be met in order to provide this level of protection against loss of deleted items:

- The Allow Purge of Items Not Backed Up option must be deselected in ConsoleOne, as described in "Modifying Environment Options" on page 977.
- User databases (user*xxx*.db) must be time-stamped every time a backup is performed so that items can be purged only after being backed up.

If you use GWTSA or TSAFS on NetWare to back up user databases, the backup time stamp is automatically added as part of the backup process. However, if you do not use GWTSA or TSAFS, you must use GWTMSTMP to make sure that user databases are time-stamped so that items will not be prematurely purged.

Restore

If you use the GWTSA or TSAFS on NetWare to restore a mailbox, the restore time stamp is automatically added as part of the restore process. However, if you do not use GWTSA or TSAFS, you can use GWTMSTMP to add the restore time stamp to the database. The restore time stamp is not required for any GroupWise feature to work properly. Its primary purpose is informational.

Retention

If you use a message retention application (see Chapter 33, "Retaining User Messages," on page 387), the application should automatically add the retention time stamp after retaining the database's messages. Any messages with dates that are newer than the retention time stamp cannot be purged from the database.

You can also use GWTMSTMP to manually add a retention time stamp.

Running GWTMSTMP on NetWare

The GWTMSTMP program (gwtmstmp.nlm) is installed into the same directory where you installed the GroupWise agents (POA and MTA). You can copy it to additional locations if needed.

To check the existing time stamp on all GroupWise user databases in a post office, use the following command:

Syntax:

```
gwtmstmp.nlm /ph-volume:\post_office_directory
```

Example:

```
gwtmstmp.nlm /ph-sys:\gwsystem\dev
```

The results are written to the console.log file.

To set a current time stamp on all user databases in a post office, use the following command:

Syntax:

```
gwtmstmp.nlm /ph-volume:\post_office_directory /set
```

Example:

```
gwtmstmp.nlm /ph-sys:\gwsystem\dev /set
```

A basic backup time stamp can also be set in ConsoleOne. Select a Post Office object, then click Tools > GroupWise Utilities > Backup/Restore Mailbox. On the Backup tab, select Backup, then click Yes.

More specialized functionality is provided through additional GWTMSTMP startup switches. See "GWTMSTMP Startup Switches" on page 408.

Running GWTMSTMP on Linux

The GWTMSTMP executable (gwtmstmp) is installed into the bin and lib subdirectories of /opt/novell/groupwise/agents along with the GroupWise agents (POA and MTA). You can copy it to additional locations if needed.

To check the existing time stamp on all GroupWise user databases in a post office, use the following command:

Syntax:

```
./gwtmstmp -p /post_office_directory
```

Example:

```
./gwtmstmp -p /gwsystem/acct
```

The results are displayed on the screen.

To set a current time stamp on all user databases in a post office, use the following command:

Syntax:

```
./gwtmstmp -p /post_office_directory --set
```

Example:

```
./gwtmstmp -p /gwsystem/acct --set
```

A basic backup time stamp can also be set in ConsoleOne. Select a Post Office object, then click Tools > GroupWise Utilities > Backup/Restore Mailbox. On the Backup tab, select Backup, then click Yes.

More specialized functionality is provided through additional GWTMSTMP startup switches. See "GWTMSTMP Startup Switches" on page 408.

Running GWTMSTMP on Windows

The GWTMSTMP program file (gwtmstmp.exe) is installed into the same directory where you installed the GroupWise agents (POA and MTA). You can copy it to additional locations if needed.

To check the existing time stamp on all GroupWise user databases in a post office, use the following command:

Syntax:

```
gwtmstmp.exe /ph-drive:\post_office_directory
```

Example:

```
gwtmstmp.exe /ph-m:\gwsystem\acct
```

The results are displayed on the screen

To set a current time stamp on all user databases in a post office, use the following command:

Syntax:

```
gwtmstmp.exe /ph-drive:\post_office_directory /set
```

Example:

```
gwtmstmp.exe /ph-m:\gwsystem\acct /set
```

A basic backup time stamp can also be set in ConsoleOne. Select a Post Office object, then click Tools > GroupWise Utilities > Backup/Restore Mailbox. On the Backup tab, select Backup, then click Yes.

More specialized functionality is provided through additional GWTMSTMP startup switches.

GWTMSTMP Startup Switches

The following startup switches can be used with GWTMSTMP:

NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
/ph	-p	/ph
/backup	-b or --backup	/backup
/restore	-r or --restore	/restore
/retention	-n or --retention	/retention
/get	-g or --get	/get
/set	-s or --set	/set
/clear	-c or --clear	/clear
/date	-d or --date	/date
/time	-t or --time	/time
/@u	-u or -userid	/@u
/userdb	-e or --userdb	/userdb

/ph

Specifies the post office directory where the user databases to time-stamp are located. This switch is required.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/ph-*volume*:\post_office_dir	-p /*post_office_dir*	/ph-*drive*:\post_office_dir
Example:	/ph-mail:\dev	-p /gwsystem/dev	/ph-j:\dev

/backup, /restore, and /retention

Specifies the time stamp on which to perform the operation. If no time stamp is specified, the operation is performed on the backup time stamp.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/backup	-b --backup	/backup
	/restore	-r --restore	/restore
	/retention	-n --retention	/retention

For example, to set the restore time stamp, you would use:

NetWare:	gwtmstmp /ph-j:\dev /restore /set
Linux:	./gwtmstmp -p /gwsystem/dev -r -s
Windows:	gwtmstmp /ph-j:\dev /restore /set

/get

Lists existing backup, restore, and retention time stamp information for user databases. If no time stamps are set, no times are displayed.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/get	-g --get	/get

For example:

NetWare:	gwtmstmp /ph-j:\dev /get
Linux:	./gwtmstmp -p /gwsystem/dev -g
Windows:	gwtmstmp /ph-j:\dev /get

If no other operational switch is used, /get is assumed. The following example returns the same results as the above example:

NetWare:	gwtmstmp /ph-j:\dev
Linux:	./gwtmstmp -p /gwsystem/dev
Windows:	gwtmstmp /ph-j:\dev

/set

Sets the current date and time on user databases.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/set	-s --set	/set

For example, to set the backup time stamp, you would use:

NetWare:	gwtmstmp /ph-j:\dev /backup /set
Linux:	./gwtmstmp -p /gwsystem/dev -b -s
Windows:	gwtmstmp /ph-j:\dev /backup /set

or

NetWare:	gwtmstmp /ph-j:\dev /set
Linux:	./gwtmstmp -p /gwsystem/dev -s
Windows:	gwtmstmp /ph-j:\dev /set

-c, --clear

Clears existing time stamps.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/clear	-c --clear	/clear

For example, to clear all time stamps on databases in a post office, you would use:

NetWare:	gwtmstmp /ph-j:\dev /clear
Linux:	./gwtmstmp -p /gwsystem/dev -c
Windows:	gwtmstmp /ph-j:\dev /clear

/date

Specifies the date that you want placed on user databases.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/date-*mm*/*dd*/*yyyy*	-d *mm*/*dd*/*yyyy* --date *mm*/*dd*/*yyyy*	/date-*mm*/*dd*/*yyyy*
Example:	/date-01/03/2004	-d 05/18/2004 --date 05/18/2004	/date-04/12/2004

For example, to set the restore date to June 15, 2004, you would use:

```
NetWare:    gwtmstmp /ph-j:\dev /restore /date-06/14/2004
Linux:      ./gwtmstmp -p /gwsystem/dev --restore --date 06/15/2004
Windows:    gwtmstmp /ph-j:\dev /restore /date-06/14/2004
```

/time

Specifies the time that you want placed on user databases.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/time-*hh*:*mm* am|pm	-t *hh*:*mm* am|pm --time *hh*:*mm* am|pm	/time-*hh*:*mm* am|pm
Example:	/time-11:30pm	-t 2:00am --time 2:00am	/time-6:15pm

For example, to set the restore time to 4:45 p.m., you would use:

```
NetWare:    gwtmstmp /ph-j:\dev /restore /time-4:45pm
Linux:      ./gwtmstmp -p /gwsystem/dev -r -t 4:45pm
Windows:    gwtmstmp /ph-j:\dev /restore /time-4:45pm
```

/@u

Provides a specific GroupWise user ID so that an individual user database can be time-stamped.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/@u-*userID*	-u *userID* --userid *userID*	/@u-*userID*
Example:	/@u-khuang	-u sjones --userid gsmith	/@u-mbarnard

For example, to set the retention time stamp for a user whose GroupWise user ID is mpalu, you would use:

```
NetWare:    gwtmstmp /ph-j:\dev /@u-mpalu /retention /set
Linux:      ./gwtmstmp -p /gwsystem/dev -u mpalu -n -s
Windows:    gwtmstmp /ph-j:\dev /@u-mpalu /retention /set
```

-e, --userdb

Provides a specific GroupWise user database (user*xxx*.db) so that an individual user database can be time-stamped.

	NetWare GWTMSTMP	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	/userdb *user_database*	-e *user_database* --userdb *user_database*	/userdb *user_database*
Example:	/userdb user3gh.db	-e user3gh.db --userdb user3gh.db	/userdb user3gh.db

For example, to set the retention time stamp for a user whose user database is named user3gh, you would use:

NetWare:	gwtmstmp /ph-j:\dev /userdb user3gh.db /retention /set
Linux:	./gwtmstmp -p /gwsystem/dev -e user3gh.db -n -s
Windows:	gwtmstmp /ph-j:\dev /userdb user3gh.db /retention /set

GroupWise Database Copy Utility

The GroupWise Database Copy utility (DBCopy) copies files from a live GroupWise post office or domain to a static location for backup. During the copy process, DBCopy prevents the files from being modified, using the same locking mechanism used by other GroupWise programs that access databases. This ensures that the backed-up versions are consistent with the originals even when large databases take a substantial amount of time to copy.

DBCopy is included in GroupWise 6.5 for Linux to assist with backing up your GroupWise system. DBCopy is available for use on NetWare and Windows servers, but it is not included in GroupWise 6.5 or 6.0.

- "Using DBCopy on Linux Servers" on page 412
- "Using DBCopy on NetWare and Windows Servers" on page 413

Using DBCopy on Linux Servers

1. Change to the directory where the DBCopy RPM is located or copy it to a convenient location on your workstation.

   The DBCopy RPM (groupwise-dbcopy-6.5.2-*mmdd*.i386.rpm is located in the /admin directory in your GroupWise software distribution directory if you have created one or on the *GroupWise 6.5 for Linux Administrator* CD.

2. Install DBCopy.

   ```
   rpm -i groupwise-dbcopy-6.5.2-mmdd.i386.rpm
   ```

3. Change to the /opt/novell/groupwise/agents/bin directory.

4. Use the following command to back up a post office:

   ```
   ./dbcopy /post_office_directory /destination_directory
   ```

   or

   Use the following command to back up a domain:

   ```
   ./dbcopy /domain_directory /destination_directory
   ```

You can also include the -I switch to specify a date (for example, 11-25-2005) so that only files that are newer than the specified date are copied.

5. After DBCopy has finished copying the post office or domain, use your backup software of choice to back up the static copy of the post office or domain directory structure.
6. After the backup has finished, delete the static copy of the post office or domain directory structure to conserve disk space.

You might find it helpful to set up a cron job to run DBCopy regularly at a time of day when your system is not busy.

DBCopy can also be useful for moving domains and post office from NetWare or Windows to Linux. For more information, see "Moving Your Existing GroupWise System to Linux" in "Update" in the *GroupWise 6.5 Installation Guide*.

Using DBCopy on NetWare and Windows Servers

For information about using DBCopy to back up GroupWise post offices on NetWare and Windows servers, see the following TIDs in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp):

- TID 10023756: Questions and Answers Regarding DBCopy
- TID 2929217: GroupWise Backup Utilities (includes Windows download)

IX Post Office Agent

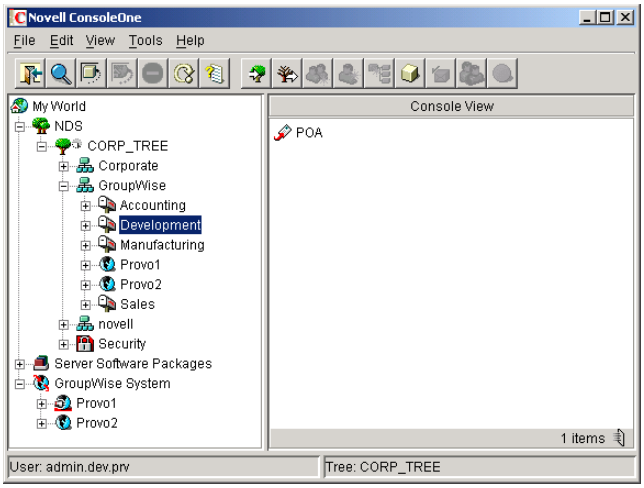
35 Understanding Message Delivery and Storage in the Post Office

A post office is a collection of user mailboxes and GroupWise® objects. Messages are delivered into mailboxes by the Post Office Agent (POA). The following topics help you understand the post office and the functions of the POA:

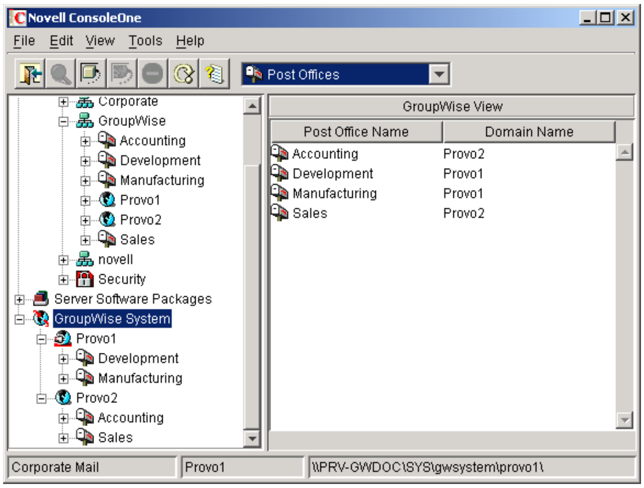
- "Post Office Representation in ConsoleOne" on page 417
- "Post Office Directory Structure" on page 418
- "Information Stored in the Post Office" on page 418
- "Post Office Access Mode" on page 422
- "Role of the Post Office Agent" on page 423
- "Message Flow in the Post Office" on page 425
- "Cross-Platform Issues in the Post Office" on page 425

Post Office Representation in ConsoleOne

In ConsoleOne®, post offices are container objects that contain at least one POA object, as shown below:



Although each post office is linked to a domain, it does not display as subordinate to the domain in the Console View. However, using the GroupWise View, you can display post offices as subordinate to the domains to which they are linked in your GroupWise system.



Post Office Name	Domain Name
Accounting	Provo2
Development	Provo1
Manufacturing	Provo1
Sales	Provo2

Post Office Directory Structure

Physically, a post office consists of a set of directories that house all the information stored in the post office. See "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Information Stored in the Post Office

The following types of information are stored in the post office:

- "Post Office Database" on page 418
- "Message Store" on page 418
- "Guardian Database" on page 420
- "Agent Input/Output Queues in the Post Office" on page 421
- "Libraries (optional)" on page 422

All databases in the post office should be backed up regularly. How often you back up GroupWise databases depends on the reliability of your network and hardware. See "Backing Up a Post Office" on page 375.

Post Office Database

The post office database (wphost.db) contains all administrative information for the post office, including a copy of the GroupWise Address Book. This information is necessary for users to send messages to others in the GroupWise system.

Message Store

GroupWise messages are made up of three parts:

- **Message Header:** The message header contains addressing information including the sender's address, recipient's address, message priority, status level, and a pointer that links the header to the message body.

- **Message Body:** The message body contains the message text in an encrypted format and a distribution list containing user IDs of the sender and recipients.
- **File Attachments (optional):** File attachments can be any type of file that is attached to the message.

The message store consists of directories and databases that hold messages. The message store is shared by all members of the post office so only one copy of a message and its attachments is stored in the post office, no matter how many members of the post office receive the message. This makes the system more efficient in terms of message processing, speed, and storage space.

All information in the message store is encrypted to prevent unauthorized access. For more information, see "Native GroupWise Encryption" on page 1039.

The message store contains the following components:

- "User Databases" on page 419
- "Message Databases" on page 419
- "Attachments Directory" on page 420

User Databases

Each member of the post office has a personal database (user*xxx*.db) which represents the user's mailbox. The user database contains the following:

- Message header information
- Pointers to messages
- Personal groups
- Personal address books
- Rules
- Contacts
- Checklists
- Categories
- Junk Mail lists

When a member of another post office shares a folder with one or more members of the local post office, a "prime user" database (pu*xxxxx*.db) is created to store the shared information. The "prime user" is the owner of the shared information.

Local user databases and prime user databases are stored in the ofuser directory in the post office.

Message Databases

Each member of the post office is arbitrarily assigned to a message database (msg*nn*.db) where the body portions of messages are stored. Many users in a post office share a single message database. There can be as many as 25 message databases in a post office. Message databases are stored in the ofmsg directory in the post office.

Outgoing messages from local senders are stored in the message database assigned to each sender. Incoming messages from users in other post offices are stored in the message database that corresponds to the message database assigned to the sender in his or her own post office. In each case, only one copy of the message is stored in the post office, no matter how many members of the post office it is addressed to.

Attachments Directory

The attachments directory (offiles) contains subdirectories that store file attachments, message text, and distribution lists that exceed 2 KB. Items of this size are stored more efficiently as files than as database records. The message database contains a pointer to where each item is found.

Guardian Database

The guardian database (ngwguard.db) serves as a reference for the following subordinate databases in the post office:

- User databases (user*xxx*.db)
- Message databases (msg*nn*.db)
- Prime user databases (pu*xxxxx*.db)
- Library databases (dmsh.db and dm*xxnn01-FF*.db)

The guardian database stores information that is common among all databases, thus eliminating duplication of information. The subordinate databases reference information stored in the guardian database. The benefits of the guardian database include the following:

- **Single Reference Point:** The guardian database stores information for each post office. Instead of storing the dictionary information in multiple dictionary databases, it is stored once in the guardian database.
- **Increased Performance:** When the information in the guardian database is accessed, it is written to cache memory. Each subsequent request can be handled with information already available in cache memory, which is faster than disk access.
- **Tracking Attachments and Documents:** When an attachment or document becomes orphaned (loses pointers to the message or profile), the guardian database is used to re-locate the origination of the attachment or document.
- **GroupWise Remote Client Management:** When a user starts the GroupWise client in Remote mode, a local guardian database is created on the user's workstation to store information similar to the guardian database in the remote user's post office in the GroupWise system.

The guardian database is vital to GroupWise functioning. Therefore, the POA has an automated back-up and roll-forward process to protect it. The POA keeps a known good copy of the guardian database called ngwguard.fbk. Whenever it modifies the ngwguard.db file, the POA also records the transaction in the roll-forward transaction log called ngwguard.rfl. If the POA detects damage to the ngwguard.db file on startup or during a write transaction, it goes back to the ngwguard.fbk file (the "fall back" copy) and applies the transactions recorded in the ngwguard.rfl file to create a new, valid and up-to-date ngwguard.db.

In addition to the POA back-up and roll-forward process, you should regularly back up the ngwguard.db, ngwguard.fbk, and ngwguard.rfl files regularly to protect against media failure. Without a valid ngwguard.db file, you cannot access your e-mail. With current ngwguard.fbk and ngwguard.rfl files, you can rebuild a valid ngwguard.db file should the need arise. See "Backing Up a Post Office" on page 375.

The ngwguard.dc file is the structural template for building the guardian database and its subordinate databases. Also called a dictionary file, the ngwguard.dc file contains schema extension information, such as administrator-defined fields, data types, and record indexes. If this dictionary file is missing, no additional databases can be created in the post office.

Agent Input/Output Queues in the Post Office

Each post office contains agent input/output queues where messages are deposited and picked up for processing by the POA and the MTA. The MTA transfers messages into and out of the post office, while the POA handles message delivery.

For illustrations of the processes presented below, see "Message Delivery to a Different Post Office" and "Message Delivery to a Different Domain" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

MTA Output Queue in the Post Office

The MTA output queue in each post office is the *post_office*\wpcsout directory.

If the MTA has a mapped or UNC link to the post office, the MTA writes user messages directly into its output queue, which requires write access to the post office. If the MTA has a TCP/IP link to the post office, the MTA transfers user messages to the POA by way of TCP/IP. The POA then stores the messages in the MTA output queue on behalf of the MTA, so the MTA does not need write access to the post office.

The *post_office*\wpcsout\ofs subdirectory is where the MTA transfers user messages for delivery by the POA to users' mailboxes in the local post office.

The MTA *post_office*\wpcsout\ads subdirectory is where the MTA transfers administrative messages instructing the POA admin thread to update the post office database (wphost.db).

POA Input Queue in the Post Office

The POA input queue in each post office is the *post_office*\wpcsout directory, which is the same as the MTA output queue.

The *post_office*\wpcsout\ofs subdirectory is where the POA picks up user messages deposited there by the MTA and updates the local message store, so users receive their messages.

The *post_office*\wpcsout\ads subdirectory is where the POA admin thread picks up administrative messages deposited there by the MTA and updates the post office database (wphost.db).

POA Output Queue in the Post Office

The POA output queue (*post_office*\wpcsin) is where the POA deposits user messages for the MTA to transfer to other domains and post offices.

Historical Note: In earlier versions of GroupWise, the GroupWise client wrote user messages to the POA output queue when using direct access to the post office. In GroupWise 6.*x*, client/server access to the post office is the preferred method.

MTA Input Queue in the Post Office

The MTA input queue in each post office (*post_office*\wpcsin) is the same as the POA output queue. The MTA picks up user messages deposited there by the POA and transfers them to other domains and post offices.

For a mapped or UNC link between the domain and post office, the MTA requires read/write access rights to its input/output queues in the post office. For a TCP/IP link, no access rights are required because messages are communicated to the MTA by way of TCP/IP.

Libraries (optional)

A library is a collection of documents and document properties stored in a database system that can be managed and searched. You do not need to set up libraries unless you are using GroupWise Document Management Services (DMS). See "Libraries and Documents" on page 261.

Library Databases

The databases for managing libraries are stored in the gwdms directory and its subdirectories in the post office.

The dmsh.db file is a database shared by all libraries in the post office. It contains information about where each library in the post office is located.

Each library has its own subdirectory in the gwdms directory. In each library directory, the dm*xxnn01-FF*.db files contain information specific to that library, such as document properties and what users have rights to access the library.

Document Storage Areas

The actual documents in a library are not kept in the library databases. They are kept in a document storage area, which consists of a series of directories for storing document files. Documents are encrypted and stored in BLOBs (binary large objects) to make document management easier. A document, its versions, and related objects are stored together in the same BLOB.

A document storage area might be located in the post office directory structure, or in some other location where more storage space is available. If it is located in the post office, the document storage area can never be moved. Therefore, storing documents in the post office directory structure is not usually recommended. If it is stored outside the post office, document storage areas can be moved when additional disk space is required.

Post Office Access Mode

The GroupWise 6.*x* Windows client and the GroupWise 6.5 Cross-Platform client both use client/server access mode to the post office. This requires a TCP/IP connection between the GroupWise clients and the POA in order for users to access their mailboxes. Benefits of client/server access include:

- **Load Balancing:** The workload is split between the client workstation and the POA on another server. The POA can perform a processor-intensive request while the client is doing something else.
- **Database Integrity:** The GroupWise client does not need write access to databases in the post office. Therefore, client failures cannot damage databases.
- **Reduced Network Traffic:** Requests are processed on the POA server and only the results are sent back across the network to the client workstation.
- **Tighter Security:** Client users do not need to log in to the server where the post office is located. This eliminates the need for users to have write access to the post office directory.
- **Scalability:** More concurrent users can be supported in a single post office.
- **Platform Independence:** The GroupWise client on any platform can access the post office by way of TCP/IP communication with the POA.

- **Simplified Client Connections:** The GroupWise client can communicate with any POA in the GroupWise system. Any POA can then redirect the client to connect to the correct POA for the users' post office.

Historical Note: In GroupWise 5.*x*, the GroupWise client allowed the user to enter a path to the post office directory to facilitate direct access mode. The GroupWise 6.*x* client no longer offers the user that option. However, you can force the GroupWise 6.*x* client to use direct access by starting it with the /ps switch and providing the path to the post office directory. For information about alternatives to client/server access mode, see the *GroupWise 5.5 Agent Setup Guide* (http://www.novell.com/documentation/gw55/index.html).

Role of the Post Office Agent

The GroupWise Post Office Agent (POA) delivers messages to users' mailboxes, connects users to their post offices in client/server access mode, updates post office databases, indexes messages and documents, and performs other post office-related tasks.You must run at least one POA for each post office.

The following sections help you understand the various functions of the POA:

- "Client/Server Processing" on page 423
- "Message File Processing" on page 424
- "Other POA Functions" on page 424

Client/Server Processing

Using client/server access mode, the GroupWise client maintains one or more TCP/IP connections with the POA and does not access the post office directly. Consequently, the performance of the POA in responding to requests from the GroupWise client directly affects the GroupWise client's responsiveness to users. To provide the highest responsiveness to client users, you can configure a POA just to handle client/server processing. See "Configuring a Dedicated Client/Server POA" on page 510.

When using client/server access mode, the GroupWise client can be configured to control how much time it spends actually connected to the POA.

- In Online mode, the client is continuously connected.
- In Caching mode, the client connects at regular intervals to check for incoming messages and also whenever the client user sends a message. Address lookup is performed locally. Caching mode allows the POA to service a much higher number of users than Online Mode.
- In Remote mode, the client connects whenever the client user chooses, such as when using a brief modem connection to download and upload messages.

NOTE: Remote mode is not currently available in the Cross-Platform client.

For more information about the client modes available with client/server access mode, see "Using Caching Mode" and "Using Remote Mode" in the *GroupWise 6.5 Windows Client User Guide* and "Using Caching Mode" in the *GroupWise 6.5 Cross-Platform Client User Guide*.

Client/server access mode also allows users to access their GroupWise mailboxes from POP and IMAP clients, in addition to the GroupWise client. See "Supporting IMAP Clients" on page 450.

In client/server mode, the POA can provide and, if necessary, force secure SSL connections with all clients. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

Message File Processing

Messages from users in other post offices arrive in the local post office in the form of message files deposited in the POA input queue. See "Agent Input/Output Queues in the Post Office" on page 421.

The POA picks up the message files and updates all user and message databases to deliver incoming messages in the local post office. To provide timely delivery for a large volume of incoming messages, you can configure a POA just to handle message file processing. See "Configuring a Dedicated Message File Processing POA" on page 513.

Other POA Functions

In addition to client/server processing (interacting with client users) and message file processing (delivering messages), the POA:

- Performs indexing tasks for document management. See "Regulating Indexing" on page 514.
- Performs scheduled maintenance on databases in the post office. See "Scheduling Database Maintenance" on page 467.
- Monitors and manages disk space usage in the post office. See "Scheduling Disk Space Management" on page 469.
- Restricts the size of messages that users can send outside the post office. See "Restricting Message Size between Post Offices" on page 455.
- Primes users' mailboxes for Caching mode. See "Supporting Forced Mailbox Caching" on page 454.
- Performs nightly user upkeep so users do not have to wait while the GroupWise client performs it; also creates a downloadable version of the system Address Book for Remote and Caching users. See "Performing Nightly User Upkeep" on page 472.
- Provides LDAP authentication and LDAP server pooling. See "Providing LDAP Authentication for GroupWise Users" on page 461.
- Prevents unauthorized access to the post office. See "Enabling Intruder Detection" on page 465.
- Tracks the GroupWise client software in use in the post office. See "Checking What GroupWise Clients Are in Use" on page 452.
- Automatically detects and repairs invalid information in user databases (user*xxx*.db) and message databases (msg*nn*.db) for the local post office by using an efficient multi-threaded process. See "Adjusting the Number of POA Threads for Database Maintenance" on page 517.
- Automatically detects and repairs invalid information in the post office database (wphost.db).
- Automatically detects and repairs damage to the guardian database (ngwguard.db) in the post office.
- Updates the post office database whenever GroupWise users, resources, post offices, or other GroupWise objects are added, modified, or deleted.
- Replicates shared folders between post offices.
- Executes GroupWise client rules.
- Processes requests from GroupWise Remote users.

Message Flow in the Post Office

To see how messages are delivered using client/server access mode, see "Message Delivery in the Local Post Office" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Cross-Platform Issues in the Post Office

GroupWise is designed to function in a variety of environments. The GroupWise Windows client runs on the following platforms:

- Windows 98
- Windows NT/2000
- Windows 3.1 (GroupWise 5.2 and below)
- Macintosh (GroupWise 5.2 and below)
- UNIX (GroupWise 5.2 and below)

The GroupWise Cross-Platform client runs on the following platforms:

- Linux
- Macintosh

In addition, GroupWise users can access their mailboxes without using a GroupWise client through the following applications:

- GroupWise WebAccess (see "WebAccess" on page 803)
- POP and IMAP clients such as Netscape* Mail, Eudora* Pro, Microsoft Outlook, and Entourage*
- MAPI clients such as Microsoft Mail and cc:Mail*

Post offices can be located on the following platforms:

- Novell® NetWare®
- Windows NT/2000
- Linux (GroupWise 6.5 for Linux)
- UNIX (GroupWise 5.*x*)

The GroupWise agents can run on the following platforms:

- Novell NetWare
- Windows NT/2000
- Linux (GroupWise 6.5 for Linux)
- UNIX (GroupWise 5.*x*)

In general, GroupWise is most efficient if you match the agent platform with the network operating system, so the POA and the post office should be on the same platform, and the client should be on a compatible platform. Those with mixed networks might wonder what combinations are possible. You have several alternatives.

- "Client/Post Office Platform Independence through Browser Technology" on page 426
- "Client/Post Office Platform Independence through Client/Server Mode" on page 426
- "POA/Post Office Platform Dependencies Because of Direct Access Requirements" on page 426

Client/Post Office Platform Independence through Browser Technology

If your GroupWise users want to access their mailboxes through POP3 or IMAP4 clients, it makes no difference what platform their post offices are located on. However, users are limited to the client capabilities of their POP3 or IMAP4 clients.

If you install GroupWise WebAccess on a Web server, GroupWise users can still access their mailboxes through their browsers and with more native GroupWise features available. See "WebAccess" on page 803 for more information.

Client/Post Office Platform Independence through Client/Server Mode

The GroupWise 6.5 Windows client and Cross-Platform client require client/server access mode. With this configuration, it makes no difference what platform users' post offices are located on. The GroupWise client accesses the post office by communicating with the POA using TCP/IP, which is a platform-independent protocol.

POA/Post Office Platform Dependencies Because of Direct Access Requirements

The POA must have direct access to the post office directory. Therefore, the POA must be able to log in to the server where the post office is located and must be able to write to the databases and directories located in the post office.

Although the recommended configuration is for the POA and the post office to be on the same platform and preferably on the same server, some variation is possible. The table below summarizes the various combinations of POA and post office platforms and indicates which combinations work for direct access and which ones do not for GroupWise 6.*x*:

	NetWare POA	Windows POA	Linux POA	UNIX POA
Post Office on NetWare	Yes	Yes	Not supported[2]	Not supported[2]
Post Office on Windows	No[1]	Yes	Yes	Not supported[2]
Post Office on Linux	Not supported[2]	Yes	Yes	Not supported[2]
Post Office on UNIX	Not supported[2]	Not supported[2]	Yes	Supported for GroupWise 5.*x*
Post Office on Macintosh	No[3]	No[3]	No[3]	No[3]

[1] The NetWare® POA cannot service a post office on a Windows server because Windows does not support the required cross-platform connection.

[2] For these combinations, an NFS connection would be required, which is not a supported configuration for the agents. However, the agents often can work adequately in this configuration.

[3] Post offices cannot be created on Macintosh computers.

36 Installing and Starting the POA

Detailed instructions for installing and starting the POA for the first post office of a new GroupWise® system are provided in "Installing a Basic GroupWise System" in the *GroupWise 6.5 Installation Guide*. Additional agent installation and startup instructions and worksheets are available in "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

IMPORTANT: If you are installing and running the POA in a clustered GroupWise system, see the appropriate section of the GroupWise 6.5 Interoperability Guide before you install the POA:

- "Deciding How to Install and Configure the Agents in a Cluster" in "Novell Cluster Services"
- "Deciding How to Install and Configure the Agents in a Cluster" in "Microsoft Clustering Services"

This section presents some additional POA installation and startup information that might be useful as you install and start additional POAs for post offices throughout your GroupWise system.

- "Installing the POA Software" on page 427
- "Starting the POA" on page 431

Installing the POA Software

Select the platform where you have installed the POA:

- "Fine-Tuning Your NetWare POA Installation" on page 427
- "Fine-Tuning Your Linux POA Installation" on page 430
- "Fine-Tuning Your Windows POA Installation" on page 430

Fine-Tuning Your NetWare POA Installation

After initial installation, you can fine-tune your NetWare® POA installation for improved performance:

- "Recommended NetWare Server Parameters for the NetWare POA" on page 427
- "Recommended NSS Parameters for the NetWare POA" on page 428
- "Estimating NetWare POA Memory Requirements" on page 428

Recommended NetWare Server Parameters for the NetWare POA

Some default settings on the NetWare® server where the NetWare POA will run might be inadequate for configurations of more than 100 concurrent client/server user connections. For a discussion of how the POA interacts with the GroupWise client, see "Post Office Access Mode" on page 422.

If you are planning a large client/server configuration, check the NetWare server parameters where the NetWare POA will be installed to make sure they are adequate for the anticipated number of

GroupWise clients. For example, in a medium-size system of 500 users in a post office, use the following settings:

Parameter	Setting
Maximum Packet Receive Buffers	2500
Minimum Packet Receive Buffers	1000
Maximum Concurrent Disk Cache Writes	200

If you are also running the NetWare MTA on the same server, see "Recommended NetWare Server Parameters for the NetWare MTA" on page 565.

Recommended NSS Parameters for the NetWare POA

If you run the NetWare POA on NetWare 5.1 or 6.*x* Novell Storage Services™ (NSS) volumes, you can significantly improve GroupWise performance by using the following parameters and settings on the nss command in the autoexec.ncf file:

/NameCacheSize=20000
/OpenFileHashShift=15
/ClosedFileCacheSize=50000
/CacheBalance=60

The best /ClosedFileCacheSize setting for a server depends on many things, such as the amount of memory on the server, the load on the POA, and the number of other programs running on the server. For example, the 50000 setting can work well for a server that has 650 MB of memory. Experiment with various settings in order to optimize performance.

The following TID, although originally written for GroupWise 5.*x* and NetWare 5.*x*, applies to GroupWise 6.*x* and NetWare 6.*x* as well:

- **TID 10065215:** Resolving GroupWise Performance Issues with NSS Volumes

Estimating NetWare POA Memory Requirements

The amount of memory required for the NetWare POA is influenced by many factors, including:

- Number of client/server connections being supported
- Number of active client connections vs. idle connections
- Number of TCP handler threads
- Number of message handler threads
- Number of database maintenance threads

The table below provides approximate memory requirements for various POA activities. Actual numbers might vary somewhat from release to release, but the numbers provided do illustrate what activities require relatively more or less memory and what configuration options require more memory than others. This information can be used to produce a rough estimate of the memory required for your particular POA configuration. Always remember this basic rule when it comes to planning for memory: More is better.

POA Component	Approx. Memory	References
Agent engine (gwenn4.nlm)[1]	500 KB	(required)
POA (gwpoa.nlm)	320 KB	(required)
Main thread, UI, logging	500 KB	(required)
Dispatcher thread	60 KB	(required)
Message handler threads (each)[2] Startup Idle Processing	 40 KB 30 KB 2000 KB	(required for message file processing) See “Adjusting the Number of POA Threads for Message File Processing” on page 512. See also /threads.
TCP dispatch/monitor/ listener thread	100 KB	(required for client/server processing) See “Using Client/Server Access to the Post Office” on page 447.
TCP handler threads (each)[2] Startup Idle Processing	 40 KB 35 KB 2500 KB	(required for client/server processing) See “Adjusting the Number of Connections for Client/ Server Processing” on page 508. See also /tcpthreads.
Client/server connections (each) No message processing Limited processing Heavy processing	 45 KB 70 KB 155 KB	(required for client/server processing) See “Adjusting the Number of Connections for Client/ Server Processing” on page 508. See also /maxappconns and /maxphysconns.
MTP processes Scanner/listener Senders/receivers (each)	 10 KB 5 KB	(required for TCP/IP link with MTA) See “Using TCP/IP Links between the Post Office and the Domain” on page 443.
QuickFinder™ thread Building/updating indexes Compressing/combining indexes	30 KB 3000 KB 4000 KB	(required for indexing) See “Regulating Indexing” on page 514. See also /qfinterval, /qfintervalinminute, / qfbaseoffset, /qfbaseoffsetinminute, and /noqf.
Nightly User Upkeep	90 KB	(recommended) See “Performing Nightly User Upkeep” on page 472. See also /nuuoffset and /nonuu.
Remote Address Book generation	40 KB	(optional) See “Performing Nightly User Upkeep” on page 472. See also /rdaboffset and /nordab.
Auto-Date events 25 events 100 events 365 events	 1530 KB 2140 KB 7885 KB	(required; occasional, temporary usage)
Notify	30 KB	(required)

POA Component	Approx. Memory	References
Admin thread Idle Processing	 20 KB 125 KB	(required for post office database update and repair) See /noada.

[1] The Agent Engine (gwenn4.nlm) needs to be loaded only once per server, no matter how many agents (POAs, MTAs, Internet Agents, WebAccess Agents) are running on that server, as long as they are running in the same address space.

[2] By default, there are six message handler threads and six TCP handler threads, for a default total of 450 KB for handler threads.

The table below provides some very general memory figures for running both GroupWise agents on the same server.

Concurrent Users	Actual Memory Usage at Peak Time
100 active users (100-250 users in post office)	50 MB
250 active users (250-500 users in post office)	110 MB
500 active users (500-1000 users in post office)	125 MB
1000 active users (1000-2500 users in post office)	150 MB

Fine-Tuning Your Linux POA Installation

After initial installation on Linux, no fine-tuning is necessary. The POA runs very efficiently in a standard Linux installation.

Fine-Tuning Your Windows POA Installation

After initial installation, you can fine-tune your Windows POA installation for improved performance:

- "Recommended Windows Parameters" on page 430
- "Estimating Windows POA Memory Requirements" on page 430

Recommended Windows Parameters

If you are running the Windows POA for a post office located on a NetWare server, you might need to increase Maximum File Locks Per Connection from its default setting.

Estimating Windows POA Memory Requirements

Although the Windows POA memory requirements differ slightly from the NetWare POA, you can use the figures provided for the NetWare POA to see what POA processes are most memory intensive. See "Estimating NetWare POA Memory Requirements" on page 428.

Starting the POA

Select the platform where you are starting the POA:

- "Starting the NetWare POA" on page 431
- "Starting the Linux POA" on page 433
- "Starting the Windows POA" on page 434

Starting the NetWare POA

After installing the NetWare POA software, you can start the NetWare POA in several ways:

- "Manually on the Command Line" on page 431
- "With a Startup File" on page 432
- "Automatically in the autoexec.ncf File" on page 432

Manually on the Command Line

1 Go to the console of the NetWare server where the NetWare POA is installed.

or

Use Remote Console to access the server:

1a Press Alt+F1 to display the options.

1b Choose Select a Screen to View.

1c Choose System Console.

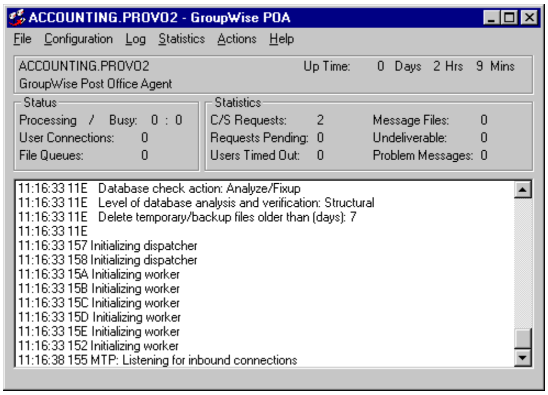
2 Enter the command to load the NetWare POA.

Syntax: `load gwpoa.nlm /home-[svr\][vol:]\po_dir`

Example: `load gwpoa.nlm /home-server1\mail:\sales`

The /home startup switch is required to start the NetWare POA. If the post office is located on a different server from where the NetWare POA is running, the /dn switch or the /user and /password switches are also required so the NetWare POA can log in to that server. You can also provide user and password information on the Post Office Settings page in ConsoleOne.

The NetWare POA agent console appears and displays normal startup status messages. See Chapter 38, "Monitoring the POA," on page 475.



```
ACCOUNTING.PROVO2                       Up Time:    0  Days  2 Hrs  9  Mins
GroupWise Post Office Agent

Processing  /  Busy:  0 : 0     C/S Requests:       2    Message Files:       0
User Connections:     0         Requests Pending:   0    Undeliverable:       0
File Queues:          0         Users Timed Out:    0    Problem Messages:    0

11:16:33 11E   Database check action: Analyze/Fixup
11:16:33 11E   Level of database analysis and verification: Structural
11:16:33 11E   Delete temporary/backup files older than (days): 7
11:16:33 11E
11:16:33 157 Initializing dispatcher
11:16:33 158 Initializing dispatcher
11:16:33 15A Initializing worker
11:16:33 15B Initializing worker
11:16:33 15C Initializing worker
11:16:33 15D Initializing worker
11:16:33 15E Initializing worker
11:16:33 152 Initializing worker
11:16:38 155 MTP: Listening for inbound connections
```

If the NetWare POA agent console does not appear, see "Post Office Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

When you start the NetWare POA as described above, it is configured according to the POA settings specified in ConsoleOne®. You can go to ConsoleOne and modify POA functioning as needed. See Chapter 37, "Configuring the POA," on page 437.

With a Startup File

Another way to start the NetWare POA is to use a startup file. You could use a startup file with the NetWare POA for the following reasons:

- Override POA settings defined in ConsoleOne.
- Control the POA locally without using ConsoleOne.
- Adjust specialized POA functions not controllable from ConsoleOne.

When you run the Agent Installation program, an initial POA startup file is created in the agent installation directory. It is named using the first 8 characters of the post office name with a .poa extension. This initial startup file includes the /home startup switch set to the location of the post office directory.

If the post office is located on a different server from where the NetWare POA is running, you must edit the startup file and provide settings for the /dn switch or the /user and /password switches so the NetWare POA can log in to that server. You can also provide user and password information on the Post Office Settings page in ConsoleOne.

The POA startup file can be modified to use other startup switches as needed. Startup switches specified on the command line override those in the startup file. Startup switches in the startup file override corresponding settings in ConsoleOne. See Chapter 40, "Using POA Startup Switches," on page 523.

When you use a startup file, you must include it on the command line when you load the NetWare POA. For example:

Syntax: `load gwpoa.nlm @`*`POA_startup_filename`*

Example: `load gwpoa.nlm @sales.poa`

In addition to the initial POA startup file, the Agent Installation program also provides a grpwise.ncf file to load the agents. If you plan to run only the NetWare POA, you should edit the grpwise.ncf file to remove the command to load the MTA.

If you run multiple NetWare POAs for the same post office, you need a startup file with the /name switch and a corresponding line in the grpwise.ncf file for each POA. A POA object in eDirectory™ is also required for each POA. See "Creating a POA Object in eDirectory" on page 438.

Automatically in the autoexec.ncf File

When the POA is running smoothly, you should modify the NetWare configuration file (autoexec.ncf) to load the NetWare POA and required NetWare programs automatically whenever you restart the server.

IMPORTANT: If you are running the POA in a Novell cluster, see "Configuring the GroupWise Volume Resource to Load and Unload the Agents" in "Novell Cluster Services" in the*GroupWise 6.5 Interoperability Guide* for alternative instructions.

1 Edit the autoexec.ncf file in the NetWare sys:\system directory.

2 Add the following command to load the agents:

```
grpwise.ncf
```

or

To start the agents in protected mode, add the following command:

```
protect grpwise.ncf
```

3 Save the autoexec.ncf file.

4 If possible, restart the server to verify that the NetWare programs and the NetWare POA are loading properly.

Starting the Linux POA

You can start the Linux POA in several ways:

- "Manually with a User Interface" on page 433
- "Manually as a Daemon" on page 433
- "Automatically at System Startup" on page 434

Manually with a User Interface

1 Make sure you are logged in as root.

2 Change to the GroupWise agent bin directory.

```
cd /opt/novell/groupwise/agents/bin
```

3 Enter the following command to start the POA:

Syntax:

```
./gwpoa --show --home post_office_directory &
```

Example:

```
./gwpoa --show --home /gwsystem/polnx &
```

The POA startup file is created by the Installation Advisor in the /opt/novell/groupwise/agents/share directory and is named after the post office that the POA services. Because the Installation Advisor prompted you for post office names and directories, it can set the --home startup switch in the POA startup file. In the bin directory where the POA executable is located, you could start the POA with a command similar to the following example:

```
./gwpoa --show @../share/lnxpost.poa
```

Manually as a Daemon

1 Make sure you are logged in as root.

2 Change to the /etc/init.d directory.

3 To start the Linux POA (and perhaps the MTA as well, depending on the configuration of the server), enter the following command:

```
./grpwise start
```

4 To confirm that the agents have started, enter the following command:

```
ps -eaf | grep gw
```

This lists all GroupWise agent process IDs.

Automatically at System Startup

If you selected Launch GroupWise Agents on System Startup in the Agent Installation program, the Agent Installation program configured your system so that the agents would start automatically each time you restart your server. The Agent Installation program always creates a grpwise startup script in /etc/init.d for starting the agents. To enable automatic startup, the Agent Installation program also creates symbolic links named S99grpwise in the rc3.d and rc5.d directories so that the agents load on restart into level 3 or 5, depending on the configuration of your Linux system.

When the grpwise script runs and starts the agents, it reads the agent startup files in /opt/novell/groupwise/agents/share to check for configuration information provided by startup switches. Because the --show switch cannot be used in the startup files, the agents never run with agent console interfaces when started automatically when the server restarts.

During agent installation, if you specified only post offices and no domains, only POA startup files were created and the grpwise startup script starts only the POA.

Starting the Windows POA

You can start the Windows POA in several ways:

- "Manually from the Windows Desktop" on page 434
- "With a Startup File" on page 434
- "Automatically in the Windows Startup Group" on page 435
- "Automatically as a Windows Service" on page 435

Manually from the Windows Desktop

In Windows, click Start > Programs > GroupWise Agents, then start the Windows POA.

The Windows POA agent console should appear and display normal startup status messages. See Chapter 38, "Monitoring the POA," on page 475.

If the Windows POA agent console does not appear, see "Post Office Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

When you start the Windows POA as described above, it is configured according to the POA settings specified in ConsoleOne. You can go back to ConsoleOne and modify POA functioning as needed. See Chapter 37, "Configuring the POA," on page 437.

With a Startup File

Another way to start the Windows POA is to use a startup file. You could use a startup file to configure the POA for the following reasons:

- Override POA settings defined in ConsoleOne.
- Control the POA locally without using ConsoleOne.
- Adjust specialized POA functions not controllable from ConsoleOne.

When you run the Agent Installation program, an initial POA startup file is created in the agent installation directory. It is named using the first 8 characters of the post office name with a .poa extension. This initial startup file includes the /home startup switch set to the location of the post office directory.

The POA startup file can be modified to use other startup switches as needed. Startup switches in the startup file override corresponding settings in ConsoleOne. See Chapter 40, “Using POA Startup Switches,” on page 523.

If you run multiple Windows POAs for the same post office, you need a startup file with the /name switch and a corresponding desktop icon or Program menu item for each one. A POA object in eDirectory is also required for each POA. See “Creating a POA Object in eDirectory” on page 438.

Automatically in the Windows Startup Group

After the Windows POA is running smoothly, you should add it to the Windows Startup group to start the Windows POA automatically whenever you restart the Windows server.

1. In Windows NT, click Start > Settings > Taskbar > Start Menu Programs > Add.

   or

   In Windows 2000, click Start > Settings > Taskbar & Start Menu > Advanced > Add.
2. Browse to the directory where you installed the Windows POA.
3. Double-click gwpoa.exe, then add the startup file to the command line.

   Example: `gwpoa.exe @sales.poa`
4. Click Next.
5. Select the Startup folder, provide a name for the shortcut, then click Finish.
6. If possible, restart the server to verify that the Windows POA starts when you log in.

Automatically as a Windows Service

To start the GroupWise Windows POA as a service for the first time after installation:

1. From the Windows desktop, click Start > Settings > Control Panel.
2. Double-click Services, select the POA service (named after the post office), then click Start.

To make sure the POA starts automatically each time you restart the server:

1. Click Start > Settings > Control Panel.
2. Double-click Services, select the POA service (named after the post office), then click Startup.
3. Select Automatic, then click OK.

   Thereafter, you can manage the Windows agents just as you would any other services.

Uninstalling the POA Software

If you move the POA to a different server, you can uninstall the POA software from the old location to regain disk space as long as the MTA is not running on the server. Select the platform where you have been running the POA:

- “Uninstalling the NetWare or Windows POA” on page 436
- “Uninstalling the Linux POA” on page 436

Uninstalling the NetWare or Windows POA

1. Stop the POA.
2. Run install.exe in the \agents subdirectory of the GroupWise software distribution directory or *GroupWise 6.5 Administrator* CD.
3. In the Install/Uninstall dialog box, click Uninstall to remove the POA software from the server.

   Windows Note: If the Windows POA was running as a service, the Agent Installation program removes the service, registry entry, and Start menu icon from Windows.

Uninstalling the Linux POA

1. Make sure you are logged in as root.
2. Stop the POA.
3. Enter the following command to determine the specific version of the POA that is running on the server:

   ```
   rpm -qa | grep groupwise
   ```

4. Enter the following command uninstall the POA:

   ```
   rpm -e novell-groupwise-agents-version-date
   ```

   where *version* is the version number (for example, 6.5.1) and *date* is the is the date when the RPM was created (for example, 0428 for April 28).

   This process removes all files and directories associated with the POA.

37 Configuring the POA

As your GroupWise® system grows and evolves, you might need to modify POA configuration to meet the changing needs of the post office it services. The following topics help you configure the POA:

Performing Basic POA Configuration

POA configuration information is stored as properties of its POA object in eDirectory. The following topics help you modify the POA object in ConsoleOne and change POA configuration to meet changing system configurations:

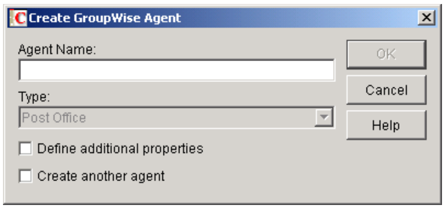
Creating a POA Object in eDirectory

When you create a new post office, one POA object is automatically created for it.You can set up additional POAs for an existing post office if message traffic in the post office is heavy. To accomplish this, you must create additional POA objects as well.

To create a new POA object in Novell® eDirectory™:

1 In ConsoleOne®, browse to and right-click the Post Office object for which you want to create a new POA object, then click New > Object.

2 Double-click GroupWise Agent to display the Create GroupWise Agent dialog box.



Agent Name:

Type: Post Office

□ Define additional properties

□ Create another agent

3 Type a unique name for the new POA. The name can include as many as 8 characters. Do not use any of the following invalid characters in the name:

- ASCII characters 0-13
- Asterisk *
- At sign @
- Braces { }
- Colon :
- Comma ,
- Double quote "
- Extended characters
- Parentheses ( )
- Period .

You use this name with the /name startup switch when you start the new POA.

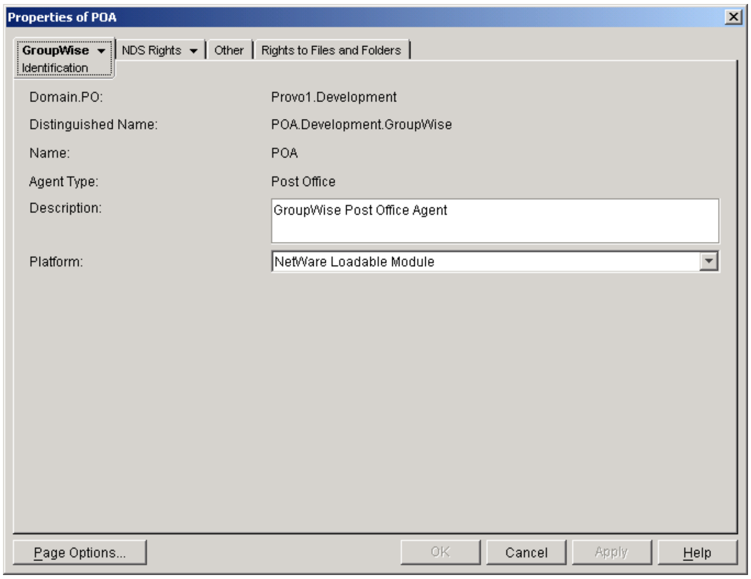
The Type field is automatically set to Post Office.

4 Select Define Additional Properties.

5 Click OK.

The POA object is automatically placed within the Post Office object.

6 Review the information displayed for the first four fields on the Identification page to ensure that you are creating the correct type of Agent object in the correct location.



Domain.PO: Provo1.Development
Distinguished Name: POA.Development.GroupWise
Name: POA
Agent Type: Post Office
Description: GroupWise Post Office Agent
Platform: NetWare Loadable Module

7 In the Description field, type one or more lines of text describing the POA.

This description displays on the POA agent console as the POA runs. When you run multiple POAs on the same server, the description should uniquely identify each one. If multiple administrators work at the server where the POA runs, the description could include a note about who to contact before stopping the POA.

8 In the Platform field, select the platform (NetWare, Linux, or Windows) where the POA will run.

9 Continue with "Configuring the POA in ConsoleOne" on page 439.

Configuring the POA in ConsoleOne

The advantage to configuring the POA in ConsoleOne, as opposed to using startup switches in a POA startup file, is that the POA configuration settings are stored in eDirectory.

1 In ConsoleOne, expand the eDirectory container where the Post Office object is located.

2 Expand the Post Office object.

3 Right-click the POA object, then click Properties.

The table below summarizes the POA configuration settings in the POA object properties pages and how they correspond to POA startup switches (as described in Chapter 40, "Using POA Startup Switches," on page 523):

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
POA Identification Page	
Domain.PO Distinguished Name Name Type Description Platform	See "Creating a POA Object in eDirectory" on page 438.

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
POA Agent Settings Page	
Message File Processing	See “Configuring a Dedicated Message File Processing POA” on page 513. See also /nomf, /nomfhigh, and /nomflow.
Message Handler Threads	See “Adjusting the Number of POA Threads for Message File Processing” on page 512. See also /threads.
Enable TCP/IP (for C/S)	See “Using Client/Server Access to the Post Office” on page 447 and “Configuring a Dedicated Client/Server POA” on page 510. See also /notcpip.
TCP Handler Threads	See “Adjusting the Number of Connections for Client/Server Processing” on page 508. See also /tcpthreads.
Max Physical Connections Max Application Connections	See “Adjusting the Number of Connections for Client/Server Processing” on page 508. See also /maxphysconns and /maxappconns.
Enable Caching	See /nocache.
CPU Utilization (NLM) Delay Time (NLM)	See “Optimizing CPU Utilization for the NetWare POA” on page 520. See also /cpu and /sleep.
Max Thread Usage for Priming and Moves	See “Supporting Forced Mailbox Caching” on page 454. See also /primingmax.
Enable IMAP Max IMAP Threads	See “Supporting IMAP Clients” on page 450. See also /imap and /imapmaxthreads.
Enable CAP Max CAP Threads	See “Supporting CAP Clients” on page 451. See also /cap and /capmaxthreads.
Enable SNMP SNMP Community "Get" String	See “Using SNMP Monitoring Programs” on page 499. See also /nosnmp.
HTTP User Name HTTP Password	See “Setting Up the POA Web Console” on page 489. See also /httpuser and /httppassword.
Network Address Page	
TCP/IP Address IPX/SPX Dress	See “Using Client/Server Access to the Post Office” on page 447 and “Using TCP/IP Links between the Post Office and the Domain” on page 443. See also /ip.
Proxy Server Address	See “Securing Client/Server Access through a Proxy Server” on page 456.
Message Transfer	See “Using TCP/IP Links between the Post Office and the Domain” on page 443. See also /mtpinipaddr, /mtpinport, /mtpoutipaddr, /mtpoutport, /mtpsendmax and /msgtranssl.

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
HTTP	See "Setting Up the POA Web Console" on page 489. See also /httpport and /httpssl.
Local Intranet Client/Server Internet Proxy Client/Server	See "Using Client/Server Access to the Post Office" on page 447 and "Using TCP/IP Links between the Post Office and the Domain" on page 443. See also /port, /internalclientssl, and /externalclientssl.
IMAP	See "Supporting IMAP Clients" on page 450. See also /imapport, /imapssl, and /imapsslport.
CAP	See "Supporting CAP Clients" on page 451. See also /capport and /capssl.
QuickFinder Page	
Enable QuickFinder Indexing Start QuickFinder Indexing QuickFinder Interval	See "Regulating Indexing" on page 514 and "Configuring a Dedicated Indexing POA" on page 516. See also /qfbaseoffset, /qfbaseoffsetinminute, /qfinterval, /qfintervalinminute, and /noqf.
Maintenance Page	
Enable Auto DB Recovery	See /norecover.
Maintenance Handler Threads	See "Adjusting the Number of POA Threads for Database Maintenance" on page 517. See also /gwchkthreads and /nogwchk.
Perform User Upkeep Start User Upkeep Generate Address Book for Remote Start Address Book Generation	See "Performing Nightly User Upkeep" on page 472. See also /nuuoffset, /nonuu, /rdaboffset, and /nordab.
Disk Check Interval Disk Check Delay	See "Scheduling Disk Space Management" on page 469.
POA Log Settings Page	
Log File Path Logging Level Max Log File Age Max Log Disk Space	See "Using POA Log Files" on page 497. See also /log, /logdays, /logdiskoff, /loglevel, and /logmax.
POA Scheduled Events Page	
Disk Check Event	See "Scheduling Disk Space Management" on page 469.
Mailbox/Library Maintenance Event	See "Scheduling Database Maintenance" on page 467.
POA SSL Settings Page	

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
Certificate File SSL Key File Password	See "Enhancing Post Office Security with SSL Connections to the POA" on page 458. See also /certfile, /keyfile, /keypassword.
Post Office Settings Page	
Remote User Name Remote Password	See Chapter 36, "Installing and Starting the POA," on page 427. See also /user and /password.
Post Office Client Access Settings Page	
Lock Out Older GroupWise Clients Minimum Client Release Version Minimum Client Release Date	See "Checking What GroupWise Clients Are in Use" on page 452. See also /gwclientreleasedate, /gwclientreleaseversion, and /enforceclientversion.
Enable Intruder Detection Incorrect Logins Allowed Incorrect Login Reset Time Lockout Reset Time	See "Enabling Intruder Detection" on page 465. See also /intruderlockout, /incorrectloginattempts, /attemptsresetinterval, and /lockoutresetinterval.
Post Office Security Page	
LDAP Authentication	See "Providing LDAP Authentication for GroupWise Users" on page 461. See also /ldapipaddr, /ldapport, /ldapuser, /ldappwd, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapssl, /ldapsslkey, and /ldaptimeout. See also /ldapippool*n*, /ldappoolresettime, /ldapportpool*n*, /ldapsslpool*n*, and /ldapsslkeypool*n*.

After you install the POA software, you can further configure the POA using a startup file. See Chapter 40, "Using POA Startup Switches," on page 523 to survey the many ways the POA can be configured.

Changing the Link Protocol between the Post Office and the Domain

How messages are transferred between the POA and the MTA is determined by the link protocol in use between the post office and the domain. For a review of link protocols, see "Link Protocols for Direct Links" on page 134.

If you need to change from one link protocol to another, some reconfiguration of the POA and its link to the domain is necessary.

- "Using TCP/IP Links between the Post Office and the Domain" on page 443
- "Using Mapped or UNC Links between the Post Office and the Domain" on page 444

NOTE: The Linux POA requires TCP/IP lines between the post office and the domain.

Using TCP/IP Links between the Post Office and the Domain

To change from a mapped or UNC link to a TCP/IP link between a post office and its domain, you must perform the following two tasks:

- "Configuring the Agents for TCP/IP" on page 443
- "Changing the Link between the Post Office and the Domain to TCP/IP" on page 443

Configuring the Agents for TCP/IP

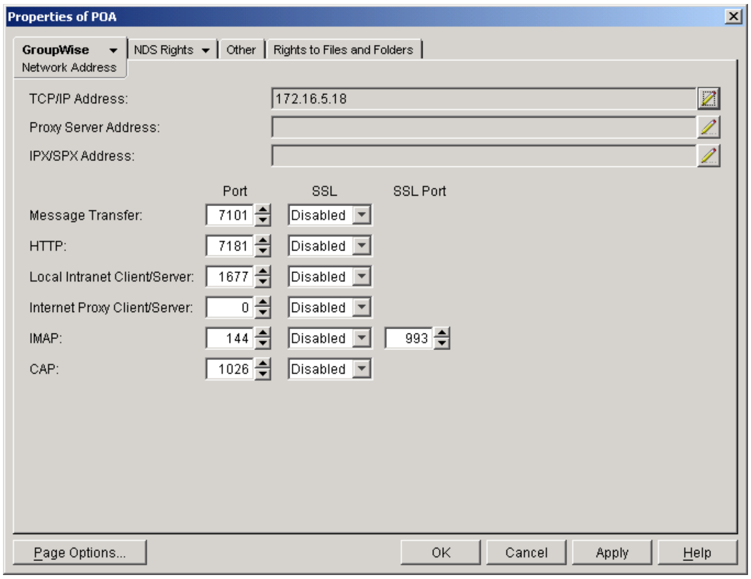
1 If the MTA in the domain is not yet set up for TCP/IP communication, follow the instructions in "Configuring the MTA for TCP/IP" on page 579.

2 To make sure the POA is properly set up for TCP/IP communication, follow the instructions in "Using Client/Server Access to the Post Office" on page 447.

Only one POA per post office needs to communicate with the MTA. If the post office has multiple POAs, have a POA that performs message file processing communicate with the MTA for best performance. For information about message file processing, see "Role of the Post Office Agent" on page 423.

3 In ConsoleOne, browse to and right-click the POA object, then click Properties.

4 Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 172.16.5.18

Proxy Server Address:

IPX/SPX Address:

	Port	SSL	SSL Port
Message Transfer:	7101	Disabled	
HTTP:	7181	Disabled	
Local Intranet Client/Server:	1677	Disabled	
Internet Proxy Client/Server:	0	Disabled	
IMAP:	144	Disabled	993
CAP:	1026	Disabled	

5 In the Message Transfer field, specify the TCP port on which the POA will listen for incoming messages from the MTA.

The default message transfer port for the POA to listen on is 7101.

6 Click OK to save the TCP/IP information and return to the main ConsoleOne window.

Corresponding Startup Switches

You could also use the /mtpinipaddr and /mtpinport startup switches in the POA startup file to set the incoming IP address and port.

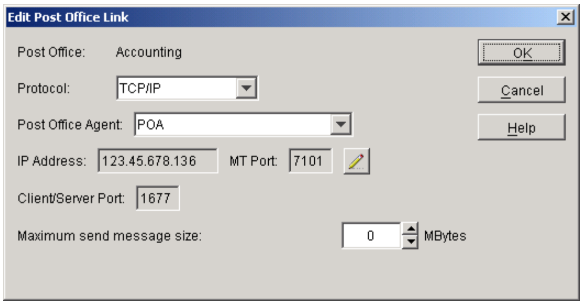
Changing the Link between the Post Office and the Domain to TCP/IP

1 In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.

2 In the drop-down list, select the domain where the post office resides.

3 Click Post Office Links, then double-click the post office for which you want to change the link protocol.

4 In the Protocol field, select TCP/IP.



Post Office: Accounting

Protocol: TCP/IP

Post Office Agent: POA

IP Address: 123.45.678.136 MT Port: 7101

Client/Server Port: 1677

Maximum send message size: 0 MBytes

5 Make sure the information displayed in the Edit Post Office Link dialog box matches the information on the Network Address page for the POA.

6 Click OK.

7 To exit the Link Configuration tool and save your changes, click File > Exit > Yes.

ConsoleOne then notifies the POA and MTA to restart using the new link protocol.

For a sample message flow for this configuration, see "TCP/IP Link Open: Transfer between Post Offices Successful" in "Message Delivery to a Different Post Office" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Corresponding Startup Switches

You could also use the /mtpoutipaddr and /mtpoutport startup switches in the POA startup file to set the outgoing IP address and port.

Using Mapped or UNC Links between the Post Office and the Domain

To change from a TCP/IP link to a mapped or UNC link between a post office and its domain:

1 In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.

2 In the drop-down list, select the domain where the post office resides.

3 Click Post Office Links, then double-click the post office for which you want to change the link protocol.

4 In the Protocol field, select Mapped or UNC.

5 Provide the location of the post office in the format appropriate to the selected protocol.

6 Click OK.

7 To exit the Link Configuration tool and save your changes, click File > Exit > Yes.

ConsoleOne then notifies the POA and MTA to restart using the new link protocol.

For a sample message flow for this configuration, see "Mapped/UNC Link Open: Transfer between Post Offices Successful" in "Message Delivery to a Different Post Office" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Moving the POA to a Different server

As your GroupWise system grows and evolves, you might need to move a POA from one server to another. For example, you might decide to run the POA on a different platform, or perhaps you want to move it to a server that has more memory.

1. When moving the POA, pay special attention to the following details:
   - For a POA configured for client/server processing, reconfigure the POA object with the new IP address and port number for the POA to use on the new server. See "Using Client/ Server Access to the Post Office" on page 447.
   - For the NetWare POA, if it was originally on the same server where the post office is located and you are moving it to a different server, add the /dn switch or the /user and /password switches to the POA startup file to give the NetWare POA access to the server where the post office is located. You can also provide user and password information on the Post Office Settings page.
2. Install the POA on the new server. See "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.
3. Start the new POA. See "Starting the POA" on page 431.
4. Observe the new POA to see that it is running smoothly. See Chapter 38, "Monitoring the POA," on page 475.
5. Stop the old POA.
6. If you are no longer using the old server for any GroupWise agents, you can remove them to reclaim the disk space. See "Uninstalling the POA Software" on page 435.

Adjusting the POA for a New Post Office Location

If you move a post office from one server to another, you also need to edit the POA startup file to provide the new location of the post office directory.

1. Stop the POA for the old post office location if it is still running.
2. Use an ASCII text editor to edit the POA startup file.

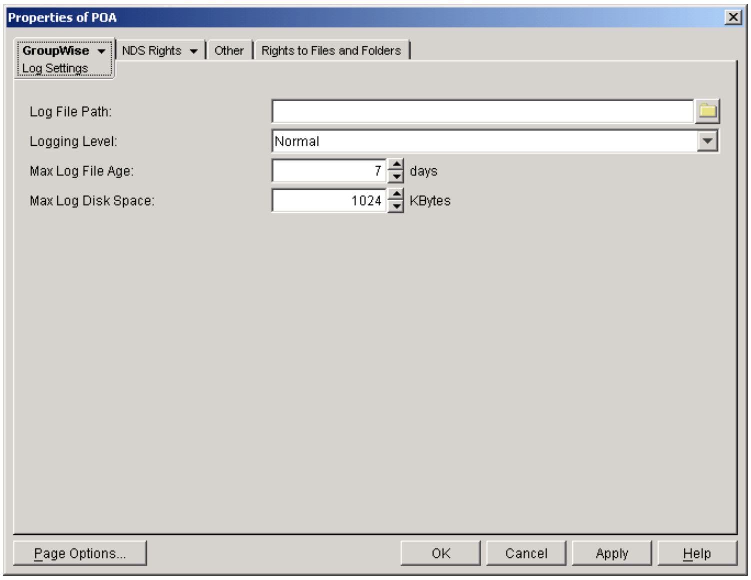
   The POA startup file is named after the post office name, plus a.poa extension.
   - On NetWare and Windows, only the first 8 characters of the post office name are used in the filename. The startup file is typically located in the directory where the POA software is installed.
   - On Linux, the full post office name is used in the filename. However, all letters are lowercase and any spaces in the post office name are removed. The startup file is located in the /opt/novell/groupwise/agents/share directory.
3. Adjust the setting of the /home switch to point to the new location of the post office directory.
4. Save the POA startup file.
5. Start the POA for the new post office location. See "Starting the POA" on page 431.
6. Adjust the link between the post office and the domain. See "Adjusting the MTA for a New Location of a Domain or Post Office" on page 587.

Adjusting the POA Logging Level and Other Log Settings

When installing or troubleshooting the POA, a logging level of Verbose can be useful. However, when the POA is running smoothly, you can set the logging level down to Normal to conserve disk space occupied by log files.

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Log Settings to display the Log Settings page.



Log File Path:

Logging Level: Normal

Max Log File Age: 7 days

Max Log Disk Space: 1024 KBytes

3 Set the desired settings for logging.

For more information about log settings and log files, see "Using POA Log Files" on page 497.

Corresponding Startup Switches
You could also use the /log, /loglevel, /logdays, /logmax, and /logdiskoff switches in the POA startup file to configure logging.

POA Web Console
You can view and search POA log files on the Log Files page.

Configuring User Access to the Post Office

As described in "Post Office Access Mode" on page 422, the GroupWise 6.*x* client defaults to client/server access mode. The following topics help you configure the POA to customize the types of client/server access provided to the post office:

- "Using Client/Server Access to the Post Office" on page 447
- "Simplifying Client/Server Access with a GroupWise Name Server" on page 449
- "Supporting IMAP Clients" on page 450
- "Supporting CAP Clients" on page 451
- "Checking What GroupWise Clients Are in Use" on page 452
- "Supporting Forced Mailbox Caching" on page 454
- "Restricting Message Size between Post Offices" on page 455

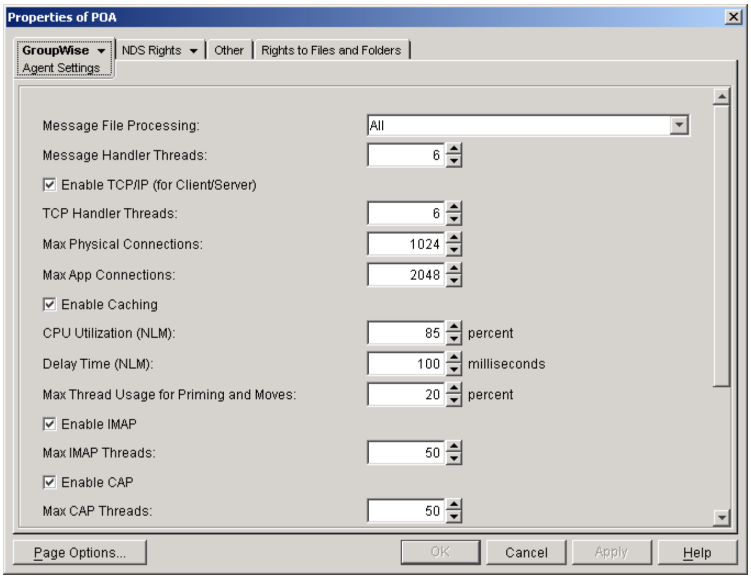
Using Client/Server Access to the Post Office

To make sure the GroupWise client has proper client/server access to the post office:

1 Make sure TCP/IP is properly set up on the server where the POA is running.

2 In ConsoleOne, browse to and right-click the POA object, then click Properties.

3 Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All

Message Handler Threads: 6

☑ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 6

Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

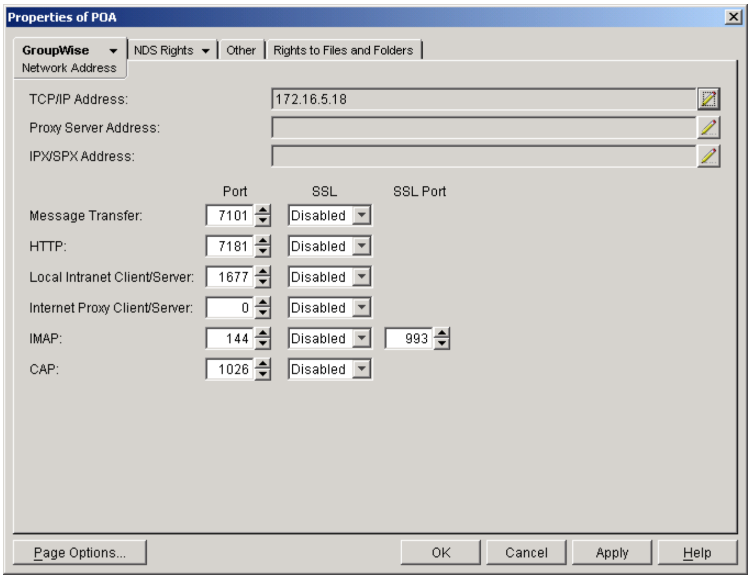
☑ Enable CAP

Max CAP Threads: 50

4 Make sure that Enable TCP/IP (for Client/Server) is selected.

The default numbers of physical connections and application connections are appropriate for a post office with as many as 500 users. If you are configuring the POA to service more than 500 users, see "Adjusting the Number of Connections for Client/Server Processing" on page 508 for more detailed recommendations. Configuring the POA with insufficient connections can result in error conditions.

5 Click GroupWise > Network Address.



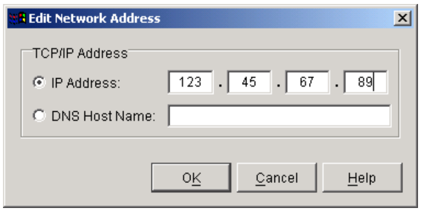
TCP/IP Address: 172.16.5.18

Proxy Server Address:

IPX/SPX Address:

	Port	SSL	SSL Port
Message Transfer:	7101	Disabled	
HTTP:	7181	Disabled	
Local Intranet Client/Server:	1677	Disabled	
Internet Proxy Client/Server:	0	Disabled	
IMAP:	144	Disabled	993
CAP:	1026	Disabled	

6 On the Network Address page, click the pencil icon for the TCP/IP Address field to display the Edit Network Address dialog box.



● IP Address: 123 . 45 . 67 . 89

○ DNS Host Name:

7 Select IP Address, then specify the IP address, in dotted decimal format, of the server where the POA is running.

or

Select DNS Host Name, then provide the DNS hostname of the server where the POA is running.

IMPORTANT: The POA must run on a server that has a static IP address. DHCP cannot be used to dynamically assign an IP address for it.

Specifying the DNS hostname rather than the IP address makes it easier to move the POA from one server to another, should the need arise at a later time. You can assign a new IP address to the hostname in DNS, without needing to change the POA configuration information in ConsoleOne.

8 Click OK.

9 To use a TCP port number other than the default port of 1677, type the port number in the Local Intranet Client/Server Port field.

If multiple POAs will run on the same server, each POA must have a unique TCP port number.

10 If needed, select Enabled or Required in the SSL drop-down list for local intranet client/server connections, Internet client/server connections, or both. For more information, see "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

11 Click OK to save the network address and port information and return to the main ConsoleOne window.

ConsoleOne then notifies the POA to restart with client/server processing enabled.

For a sample message flow for this configuration, see "Message Delivery in the Local Post Office" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Corresponding Startup Switches
You could also use the /port switch in the POA startup file to provide the client/server port number. On a server with multiple IP addresses, you can use the /ip switch to bind the POA to a specific address.

POA Web Console
You can view the TCP/IP address and port information for the POA on the Configuration page under the Client/Server Settings heading.

Simplifying Client/Server Access with a GroupWise Name Server

If GroupWise users are set up correctly in eDirectory, the GroupWise client can determine which post office to access for each user based on the information stored in eDirectory. This lets the GroupWise client start automatically in client/server mode without users needing to know and provide any IP address information. However, some GroupWise users might be on platforms where eDirectory is not in use. To fill the same function for non-eDirectory users, you can set up a GroupWise name server.

A GroupWise name server redirects each GroupWise client user to the IP address and port number of the POA that services the user's post office. By setting up a GroupWise name server, non-eDirectory GroupWise client users do not need to know and provide any IP address information when they start the GroupWise client in client/server mode. The GroupWise name server takes care of this for them.

- "Required Hostnames" on page 449
- "Required Port Number" on page 449
- "How a GroupWise Name Server Helps the GroupWise Client Start" on page 449
- "Setting Up a GroupWise Name Server" on page 450

Required Hostnames

The primary GroupWise name server must be designated using the hostname ngwnameserver. You can also designate a backup GroupWise name server using the hostname ngwnameserver2.

Required Port Number

Each server designated as a GroupWise name server must have a POA running on it that uses the default port number of 1677. Other agents can run on the same server, but one POA must use the default port number of 1677 in order for the GroupWise name server to function. For setup instructions, see "Using Client/Server Access to the Post Office" on page 447.

How a GroupWise Name Server Helps the GroupWise Client Start

After a server has been designated as ngwnameserver, and a POA using the default port number of 1677 is running on that server, the GroupWise client can connect to the POA of the appropriate post office by contacting the POA located on ngwnameserver. If ngwnameserver is not available, the client next attempts to contact the backup name server, ngwnameserver2. If no GroupWise name server is available, the user would need to provide the IP address and port number of the appropriate POA in order to start the GroupWise client in client/server mode.

Setting Up a GroupWise Name Server

1. Make sure that TCP/IP is set up and functioning on your network.
2. Know the IP address of the server you want to set up as a GroupWise name server.
3. Make sure the POA on that server uses the default TCP port of 1677.
4. If you want a backup GroupWise name server, identify the IP address of a second server where the POA uses the default TCP port of 1677.
5. Use your tool of choice for modifying DNS.

   NetWare Note: On a NetWare server, you could use INETCFG.

   Linux Note: On a SUSE server, you could use the YaST Control Center. On a Red Hat server, you could use Server Settings > Domain Name Server on the Red Hat menu.

   Windows Note: On a Windows server, you could use DNS Manager.
6. Create an entry for the IP address of the first POA and give it the hostname ngwnameserver.
7. If you want a backup name server, create an entry for the IP address of the second POA and give it the hostname ngwnameserver2.

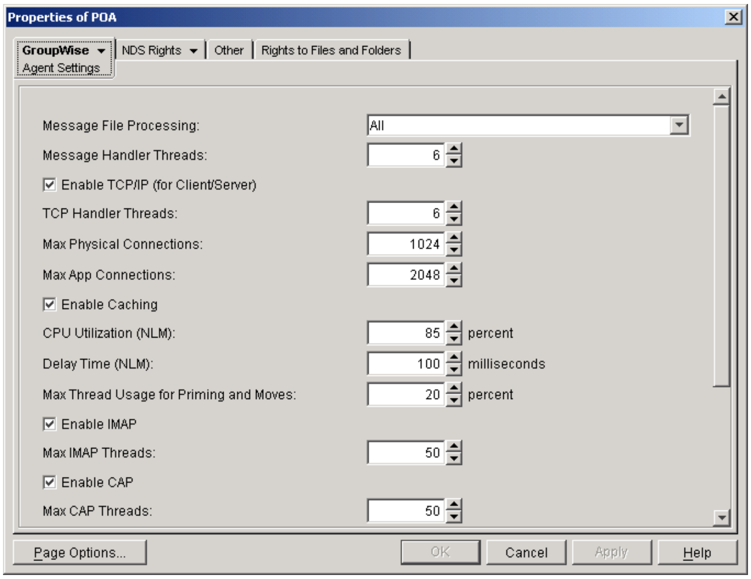
   You must use the hostnames ngwnameserver and ngwnameserver2. Any other hostnames are not recognized as GroupWise name servers.
8. Save your changes.

As soon as the hostname information replicates throughout your system, GroupWise client users can start the GroupWise client in client/server mode without specifying a TCP/IP address and port number.

Supporting IMAP Clients

You can configure the POA so that IMAP (Internet Messaging Application Protocol) clients such as Netscape Mail, Eudora Pro, Microsoft Outlook, and Entourage can connect to the post office much like the GroupWise client does.

1. In ConsoleOne, browse to and right-click the POA object, then click Properties.
2. Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All
Message Handler Threads: 6
☑ Enable TCP/IP (for Client/Server)
TCP Handler Threads: 6
Max Physical Connections: 1024
Max App Connections: 2048
☑ Enable Caching
CPU Utilization (NLM): 85 percent
Delay Time (NLM): 100 milliseconds
Max Thread Usage for Priming and Moves: 20 percent
☑ Enable IMAP
Max IMAP Threads: 50
☑ Enable CAP
Max CAP Threads: 50

3. Select Enable IMAP.

   The default maximum number of IMAP threads is 50. This is adequate for most post offices, because each IMAP thread can service multiple IMAP clients. New threads are started automatically to service clients until the maximum number is reached.

4. If you want IMAP clients to use SSL connections to the post office, click GroupWise > Network Address, then select Enabled or Required in the IMAP SSL drop-down list.

   For additional instructions about using SSL connections, see Chapter 80, “Encryption and Certificates,” on page 1039.

5. Click OK to save the IMAP settings and return to the main ConsoleOne window.

   ConsoleOne then notifies the POA to restart with IMAP enabled.

Corresponding Startup Switches

You could also use the /imap, /imapmaxthreads, /imapport, /imapssl, /imapsslport, and /imapreadlimit startup switches in the POA startup file to configure the POA to support IMAP clients.

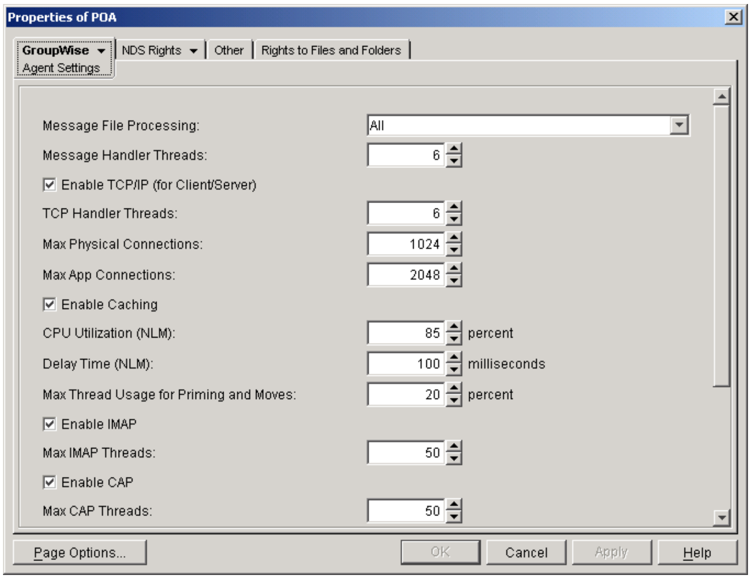
POA Web Console

You can see whether IMAP is enabled on the Configuration page under the General Settings heading.

Supporting CAP Clients

You can configure the POA so that CAP (Calendar Access Protocol) clients can connect to the post office much like the GroupWise client does.

1. In ConsoleOne, browse to and right-click the POA object, then click Properties.
2. Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All

Message Handler Threads: 6

☑ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 6

Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

☑ Enable CAP

Max CAP Threads: 50

3. Select Enable CAP.

   The default maximum number of CAP threads is 50. This is adequate for most post offices, because each CAP thread can service multiple CAP clients. New threads are started automatically to service clients until the maximum number is reached.

4. If you want CAP clients to use SSL connections to the post office, click GroupWise > Network Address, then select Enabled or Required in the CAP SSL drop-down list.

   For additional instructions about using SSL connections, see Chapter 80, “Encryption and Certificates,” on page 1039.

5. Click OK to save the CAP settings and return to the main ConsoleOne window.

   ConsoleOne then notifies the POA to restart with CAP enabled.

Corresponding Startup Switches

You could also use the /cap, /capmaxthreads, /capport, and /capssl startup switches in the POA startup file to configure the POA to support CAP clients.

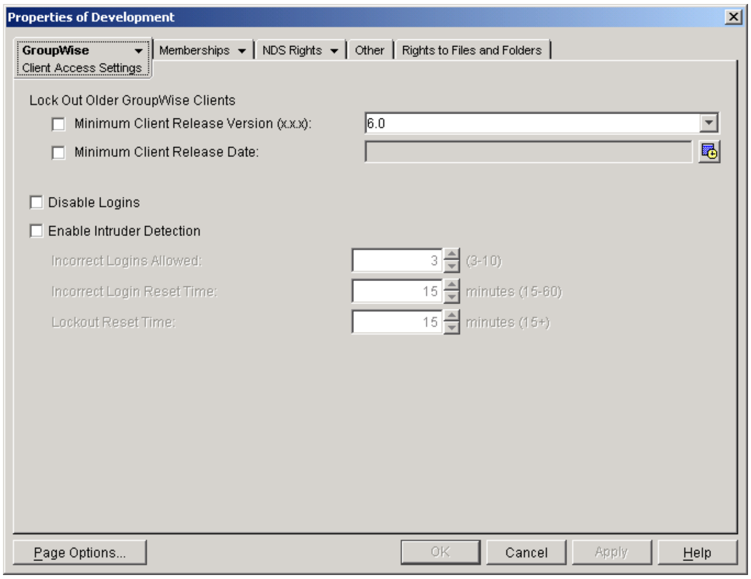
POA Web Console

You can see whether CAP is enabled on the Configuration page under the General Settings heading.

Checking What GroupWise Clients Are in Use

You can configure the POA to identify GroupWise client users who are running GroupWise clients that do not correspond to a specified release version and/or date. You can also force them to update to the specified version.

1. In ConsoleOne, browse to and right-click the Post Office object, then click Properties.
2. Click GroupWise > Client Access Settings to display the Client Access Settings page.



Lock Out Older GroupWise Clients

□ Minimum Client Release Version (x.x.x): 6.0

□ Minimum Client Release Date:

□ Disable Logins

□ Enable Intruder Detection

Incorrect Logins Allowed: 3 (3-10)

Incorrect Login Reset Time: 15 minutes (15-60)

Lockout Reset Time: 15 minutes (15+)

3 Specify the approved GroupWise release version, if any.

Only 6.*x* versions of the client are supported for lockout.

4 Specify the approved GroupWise release date, if any

You can specify the minimum version, the minimum date, or both. If you specify both minimums, any user for which both minimums are not true is identified as running an older GroupWise client.

5 Select Lock Out Older GroupWise Clients for the version and/or date if you want to force users to update in order to access their GroupWise mailboxes.

If you lock out older clients, client users receive an error message and be unable to access their mailboxes until they upgrade their GroupWise client software to the minimum required version and/or date.

6 Click OK to save the GroupWise version and/or date settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches

You could also use the /gwclientreleaseversion, /gwclientreleasedate, and /enforceclientversion startup switches in the POA startup file to configure the POA to check client version and/or date information.

POA Web Console

On the Status page of the POA Web console, click C/S Users to display the Current Users page, which lists all GroupWise users who are currently accessing the post office. Users who are running GroupWise clients older than the approved version and/or date are highlighted in red in the list.

Historical Note: The capability of identifying client version and date information was first introduced in GroupWise 5.5 Enhancement Pack Support Pack 1. Any clients with versions and dates earlier than GroupWise 5.5 Enhancement Pack Support Pack 1 do not appear at all on the Current Users page of the POA Web console.

Supporting Forced Mailbox Caching

GroupWise client users have the option to download their GroupWise mailboxes to their workstations so they can work without being continuously connected to the network. This is called Caching mode. For more information, see "Caching Mode" on page 965.

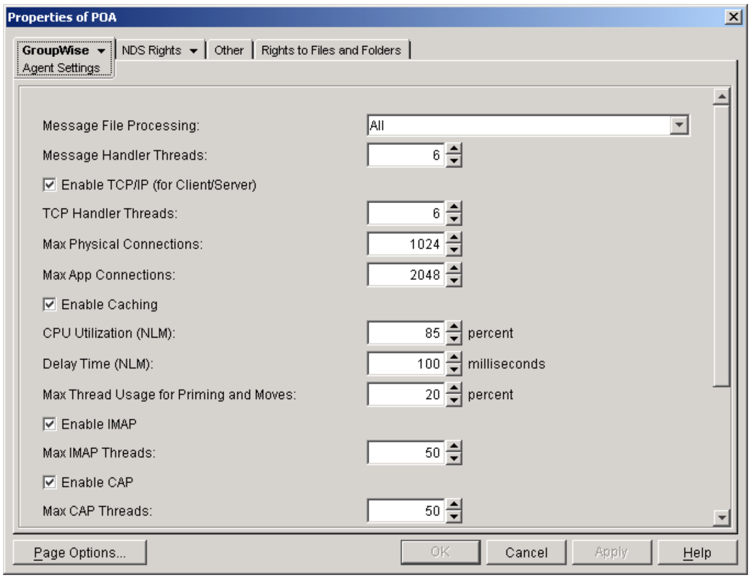
When client users change to Caching mode, the contents of their mailboxes must be copied to their hard drives. This process is called "priming" the mailbox. If users individually decide to use Caching mode, the POA easily handles the process.

If you force all users in the post office to start using Caching mode, as described in "Allowing or Forcing Use of Caching Mode" on page 966, multiple users might attempt to prime their mailboxes at the same time. This creates a load on the POA that can cause unacceptable response to other users.

To configure the POA to handle multiple requests to prime mailboxes:

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All

Message Handler Threads: 6

☑ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 6

Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

☑ Enable CAP

Max CAP Threads: 50

3 Set Max Thread Usage for Priming and Moves as needed.

By default, the POA allocates only 20% of its TCP handler threads for priming mailboxes for users who are using Caching mode for the first time. In a default configuration, this would be only one thread. You might want to specify 60 or 80 so that 60% to 80% of POA threads are used for priming mailboxes. You might also want to increase the number of TCP handler threads the POA can start in order to handle the temporarily heavy load while users are priming their mailboxes. See "Adjusting the Number of Connections for Client/Server Processing" on page 508.

4 Click OK to save the new setting.

ConsoleOne then notifies the POA to restart so the new setting can be put into effect.

Corresponding Startup Switches

You could also use the /primingmax switch in the POA startup file to configure the POA to handle multiple requests to prime mailboxes.

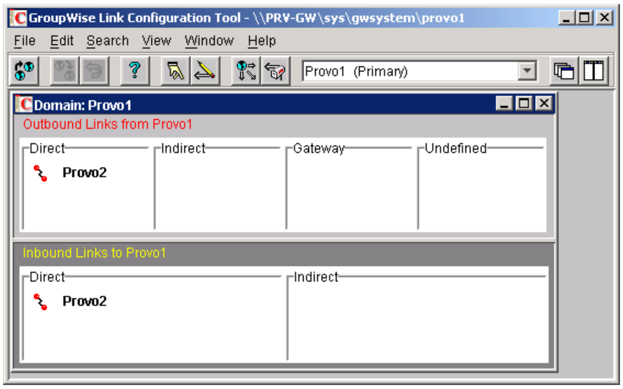
POA Web Console

You can change the POA's ability to respond to caching requests for the current POA session on the Configuration page. Under the Client/Server Settings heading, click Max Thread Usage for Priming and Live Moves. To increase the number of client/server threads, click Client/Server Processing Threads under the Performance Settings heading.

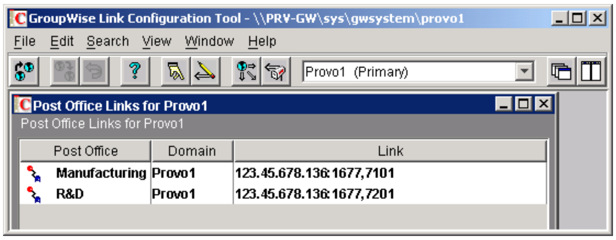
Restricting Message Size between Post Offices

You can configure the POA to restrict the size of messages that users are permitted to send outside the post office.

1 In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.

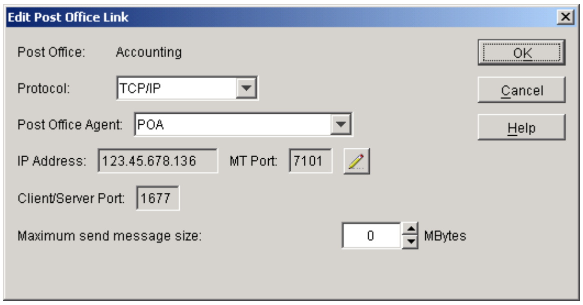


2 In the drop-down list, select the domain where the post office resides, then click Post Office Links.


GroupWise Link Configuration Tool - \\PRV-GW\sys\gwsystem\provo1
File
Edit
Search
View
Window
Help
Provo1 (Primary)
Post Office Links for Provo1
Post Office Links for Provo1

Post Office	Domain	Link
Manufacturing	Provo1	123.45.678.136:1677,7101
R&D	Provo1	123.45.678.136:1677,7201

3 Double-click the post office where you want to restrict message size.



Post Office: Accounting

Protocol: TCP/IP

Post Office Agent: POA

IP Address: 123.45.678.136 MT Port: 7101

Client/Server Port: 1677

Maximum send message size: 0 MBytes

4 In the Maximum Send Message Size field, specify in megabytes the size of the largest message you want users to be able to send outside the post office, then click OK.

5 To exit the Link Configuration tool and save your changes, click File > Exit > Yes.

ConsoleOne then notifies the POA to restart using the new maximum message size limit.

If a user's message is not sent out of the post office because of this restriction, the user receives an e-mail message with a subject line of:

```
Delivery disallowed
```

plus the subject of the original message. This message provides information to the user about why and where the message was disallowed. However, the message is still delivered to recipients in the sender's own post office.

There are additional ways to restrict the size of messages that users can send, as described in "Restricting the Size of Messages That Users Can Send" on page 175.

Corresponding Startup Switches
You could also use the /mtpsendmax startup switch in the POA startup file to restrict message size.

POA Web Console
You can view the maximum message size on the Configuration page. You can change the maximum message size for the current POA session using the Message Transfer Protocol link on the Configuration page.

Configuring Post Office Security

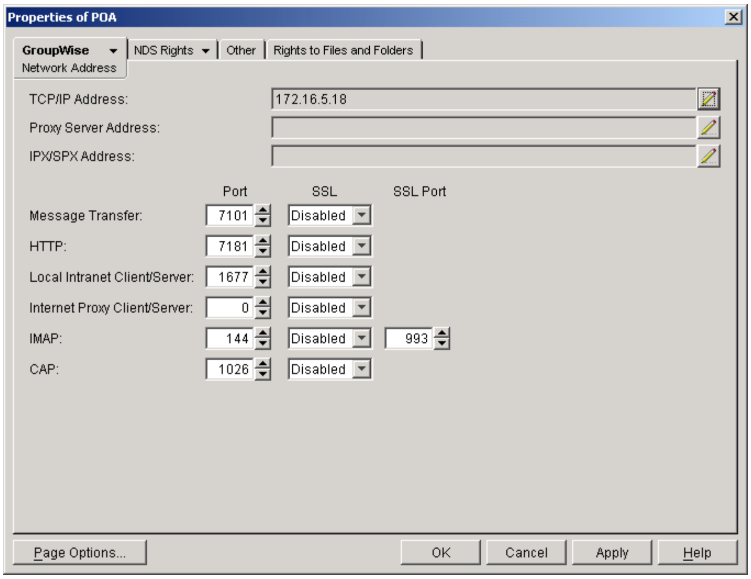
You can configure the POA in various ways to meet the security needs of the post office.

- "Securing Client/Server Access through a Proxy Server" on page 456
- "Enhancing Post Office Security with SSL Connections to the POA" on page 458
- "Providing LDAP Authentication for GroupWise Users" on page 461
- "Enabling Intruder Detection" on page 465

Securing Client/Server Access through a Proxy Server

If the server where the POA runs is behind your firewall, you can link it to a proxy server in order to provide client/server access to the post office for GroupWise client users who are outside the firewall.

1. In ConsoleOne, browse to and right-click the POA object, then click Properties.
2. Click GroupWise > Network Address to display the POA Network Address page.



TCP/IP Address: 172.16.5.18

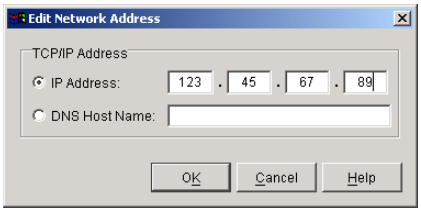
Proxy Server Address:

IPX/SPX Address:

	Port	SSL	SSL Port
Message Transfer:	7101	Disabled	
HTTP:	7181	Disabled	
Local Intranet Client/Server:	1677	Disabled	
Internet Proxy Client/Server:	0	Disabled	
IMAP:	144	Disabled	993
CAP:	1026	Disabled	

3 Make sure the POA is already configured for client/server processing as explained in "Using Client/Server Access to the Post Office" on page 447.

4 Click the pencil icon for the Proxy Server Address field to display the Edit Network Address dialog box.



● IP Address: 123 . 45 . 67 . 89

○ DNS Host Name:

5 Select IP Address, then specify the IP address, in dotted decimal format, of the server that GroupWise client users access from outside your firewall.

or

Select DNS Host Name, then provide the DNS hostname of that server.

6 Click OK.

7 If you want to use a different port number for the proxy server than you are using for client/server access to the POA itself, provide the port number in the Internet Proxy Client/Server field.

8 Click OK to save the proxy server network address and port and return to the main ConsoleOne window.

ConsoleOne then notifies the POA to restart and begin communicating with the proxy server.

POA Web Console

You can list all POAs in your GroupWise system, along with their proxy server addresses. On the Configuration page, click IP Addresses Redirection Table under the General Settings heading.

Controlling Client Redirection Inside and Outside Your Firewall

When a user tries to access his or her mailbox without providing the IP address of the POA for his or her post office, any POA or a GroupWise name server POA can redirect the request to the POA for the user's post office.

A POA that is configured with both an internal IP address and a proxy IP address automatically redirects internal users to internal IP addresses and external users to proxy IP addresses. However, if you want to control which users are redirected to which IP addresses based on other criteria than user location, you can configure a post office with one POA to always redirect users to internal IP addresses and a second POA to always redirect users to proxy IP addresses. Users are then redirected based on which POA IP address they provide in the GroupWise Startup dialog box when they start the GroupWise client to access their mailboxes.

1 Configure the initial POA for the post office with the IP address that you want for internal users. For instructions, see "Using Client/Server Access to the Post Office" on page 447.

  Do not fill in the Proxy Server Address field on the Network Address page of the POA object.

2 Create a second POA object in the post office and give it a unique name, such as POA_PRX. For instructions, see "Creating a POA Object in eDirectory" on page 438.

3 Configure this second POA with a proxy IP address. For instructions, see "Securing Client/Server Access through a Proxy Server" on page 456.

  Do not fill in the TCP/IP Address field on the Network Address page of the POA object.

4 Create a startup file for the new instance of the POA.

  4a Use the /name switch to specify the name of the POA object that you created in Step 2.

  4b Use the /ip switch to specify the IP address of the server where this instance of the POA runs.

  4c Use the /port switch to specify the client/server port that this instance of the POA listens on.

  This information needs to be specified in the POA startup file because this information is not specified in ConsoleOne for this instance of the POA.

5 Start the new instance of the POA.

6 Give users that you want to be redirected to internal IP addresses the IP address you used in Step 1.

7 Give users that you want to be redirected to proxy IP addresses the IP address you used in Step 3.

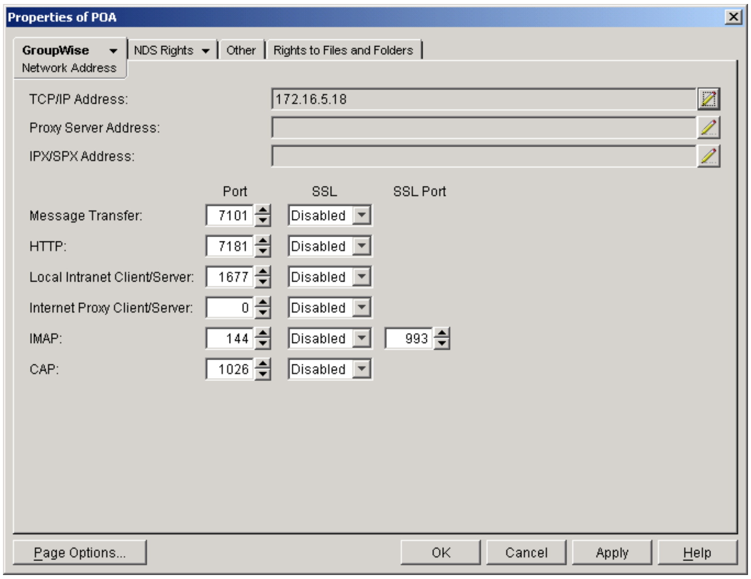
Enhancing Post Office Security with SSL Connections to the POA

Secure Sockets Layer (SSL) ensures secure communication between the POA and other programs by encrypting the complete communication flow between the programs. For background information about SSL and how to set it up on your system, seeChapter 80, "Encryption and Certificates," on page 1039.

To configure the POA to use SSL:

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 172.16.5.18

Proxy Server Address:

IPX/SPX Address:

	Port	SSL	SSL Port
Message Transfer:	7101	Disabled	
HTTP:	7181	Disabled	
Local Intranet Client/Server:	1677	Disabled	
Internet Proxy Client/Server:	0	Disabled	
IMAP:	144	Disabled	993
CAP:	1026	Disabled	

3 To use SSL connections between the POA and GroupWise clients located inside your firewall, select Enabled in the Local Intranet Client/Server SSL drop-down list to let the GroupWise client determine whether an SSL connection or non-SSL connection is used. (Non-SSL connections are still protected by native GroupWise encryption.)

or

Select Required in the Local Intranet Client/Server SSL drop-down list if you want the POA to force SSL connections, so that non-SSL connections are denied.

IMPORTANT: Clients older than GroupWise 6.5 cannot connect to the POA if SSL is required.

4 To use SSL connections between the POA and GroupWise clients located outside your firewall (for example, across the Internet), select Enabled in the Internet Client/Server SSL drop-down list to let the GroupWise client determine whether an SSL connection or non-SSL connection is used. (Non-SSL connections are still protected by native GroupWise encryption.)

or

Select Required in the Internet Client/Server SSL drop-down list if you want the POA to force SSL connections, so that non-SSL connections are denied.

IMPORTANT: Clients older than GroupWise 6.5 cannot connect to the POA if SSL is required.

5 To use SSL connections between the POA and IMAP clients, select Enabled in the IMAP SSL drop-down list to let the IMAP client determine whether an SSL connection or non-SSL connection is used.

or

Select Required in the IMAP SSL drop-down list if you want the POA to force SSL connections, so that non-SSL connections from IMAP clients are denied.

6 To use SSL connections between the POA and its MTA, select Enabled in the Message Transfer SSL drop-down list.

The POA must use a TCP/IP link with the MTA in order to enable SSL for the connection. See "Using TCP/IP Links between the Post Office and the Domain" on page 443.

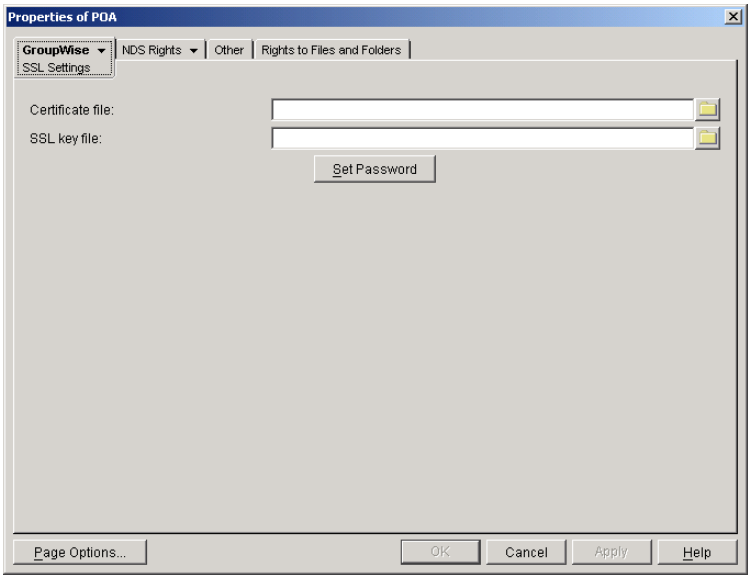
The MTA must also have SSL enabled for the connection to be secure. See "Enhancing Domain Security with SSL Connections to the MTA" on page 589. If the MTA does not have SSL enabled, the POA falls back to native GroupWise encryption.

7 To use SSL connections between the POA and the POA Web console displayed in your Web browser, select Enabled in the HTTP SSL drop-down list.

To set up the POA Web console, see "Setting Up the POA Web Console" on page 489.

8 Click Apply to save the settings on the Network Address page.

9 Click GroupWise > SSL Settings to display the SSL Settings page.



Certificate file:

SSL key file:

For background information about certificate files and SSL key files, see Chapter 80, "Encryption and Certificates," on page 1039.

By default, the POA looks for the certificate file and SSL key file in the same directory where the POA executable is located, unless you provide a full pathname.

10 In the Certificate File field, browse to and select the public certificate file provided to you by your CA.

11 In the SSL Key File field:

11a Browse to and select your private key file.

11b Click Set Password.

11c Provide the password that was used to encrypt the private key file when it was created.

11d Click Set Password.

12 Click OK to save the SSL settings.

ConsoleOne then notifies the POA to restart and access the certificate and key files.

Corresponding Startup Switches

You could also use the /certfile, /keyfile, /keypassword, /httpssl, /msgtranssl, /imapssl, and /imapsslport switches in the POA startup file to configure the POA to use SSL.

POA Web Console

You can view SSL information for the POA on the Status and Configuration pages. In addition, when you list the client/server users that are accessing the post office, SSL information is displayed for each user.

Providing LDAP Authentication for GroupWise Users

By default, GroupWise client users' passwords are stored in eDirectory and the POA authenticates users to their GroupWise mailboxes through eDirectory. For background information about passwords, see Chapter 79, "GroupWise Passwords," on page 1033.

By enabling LDAP authentication for the POA, users' password information can be retrieved from any network directory that supports LDAP. For background information about LDAP, see "Authenticating to GroupWise with Passwords Stored in an LDAP Directory" on page 1047.

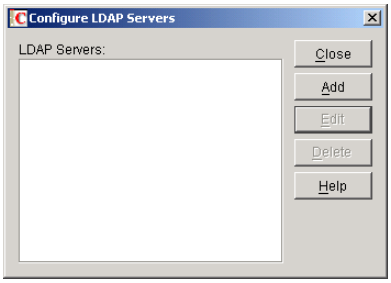
When you enable LDAP authentication, it is important to provide fast, reliable access to the LDAP directory because GroupWise client users cannot access their mailboxes until they have authenticated. The following sections provide instructions for configuring the POA to make the most efficient use of the LDAP servers available on your system:

- "Providing LDAP Server Configuration Information" on page 461
- "Enabling LDAP Authentication for a Post Office" on page 462
- "Configuring a Pool of LDAP Servers" on page 464
- "Specifying Failover LDAP Servers (Non-SSL Only)" on page 465

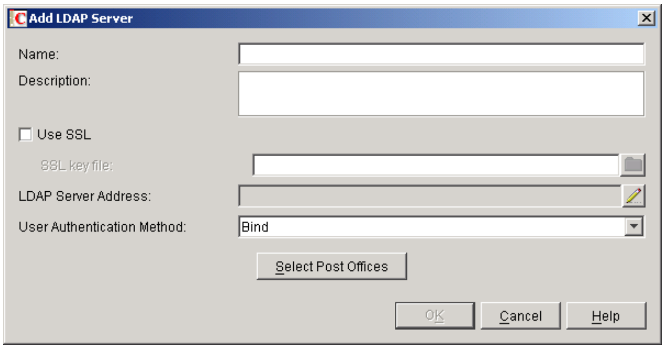
Providing LDAP Server Configuration Information

Information about your available LDAP servers must be provided in ConsoleOne before you can enable LDAP authentication for users.

1. In ConsoleOne, click Tools > GroupWise System Operations > LDAP Servers to display the Configure LDAP Servers dialog box.



2. Click Add to add an LDAP server and provide configuration information about it.



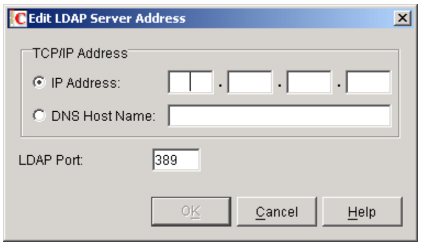
□ Use SSL

User Authentication Method: Bind

3. In the Name field, type the name by which you want the LDAP server to be known in your GroupWise system.
4. In the Description field, provide additional information about the LDAP server as needed.
5. If the LDAP server requires an SSL connection, select Use SSL, then browse to and select the SSL key file, as provided by the LDAP server.

   For additional instructions about using SSL connections, see the following resources:

   - Authentication and Security (http://www.novell.com/documentation/edir873/edir873/data/agtxhz5.html#agtxhz5)
   - Enabling LDAP Authentication with GroupWise (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10067375.htm)
6. Click the pencil icon for the LDAP Server Address field.


Edit LDAP Server Address

TCP/IP Address

● IP Address: . . .

○ DNS Host Name:

LDAP Port: 389

7. Select IP Address, then specify the IP address, in dotted decimal format, of the LDAP server.

   or

   Select DNS Host Name, then provide the DNS hostname of the LDAP server.

   The default LDAP port is 389 for non-SSL connections and 636 for SSL connections.
8. If the default port number is already in use, specify a unique LDAP port number.
9. Click OK to save the LDAP server address and port information.
10. In the User Authentication Method field, select Bind or Compare.

    For a comparison of these methods, see "Authenticating to GroupWise with Passwords Stored in an LDAP Directory" on page 1047.
11. Click OK to save the configuration information for the LDAP server.
12. Repeat Step 2 through Step 11 for each LDAP server that you want to make available to GroupWise for LDAP authentication.

    Providing configuration information for multiple LDAP servers creates a pool of LDAP servers, which provides fault tolerance and load balancing to ensure fast, reliable mailbox access for GroupWise users.
13. Continue with "Enabling LDAP Authentication for a Post Office" on page 462

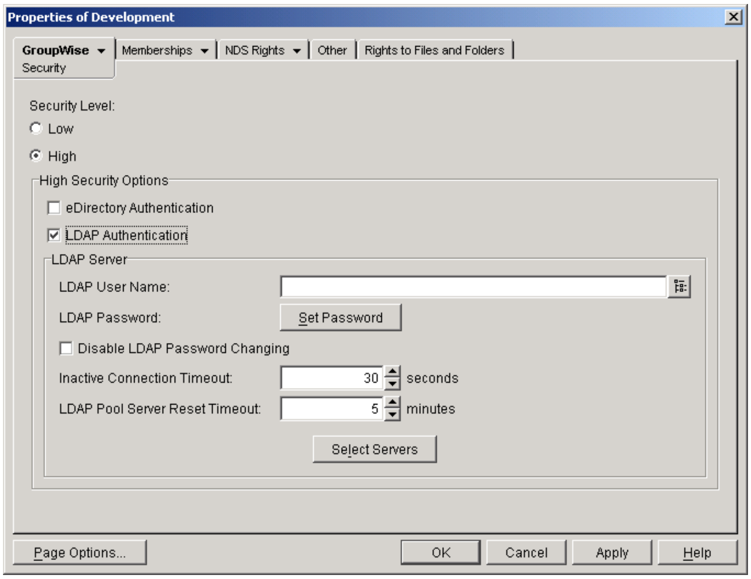
Corresponding Startup Switches
You could also use the /ldapipaddr, /ldapport, /ldapuserauthmethod, /ldapssl, and /ldapsslkey startup switches in the POA startup file to provide the LDAP server information.

Enabling LDAP Authentication for a Post Office

To configure the POA to perform LDAP authentication for the users in a post office:

1. In ConsoleOne, browse to and right-click the Post Office object, then click Properties.

2 Click GroupWise > Security to display the Security page.



Security Level:

○ Low

● High

High Security Options

□ eDirectory Authentication

☑ LDAP Authentication

LDAP Server

LDAP User Name:

LDAP Password: Set Password

□ Disable LDAP Password Changing

Inactive Connection Timeout: 30 seconds

LDAP Pool Server Reset Timeout: 5 minutes

3 For Security Level, select High.

4 In the High Security Options box, select LDAP Authentication.

5 If you want the POA to access the LDAP server with specific rights to the LDAP directory, specify a username that has those rights.

If you are using a Novell LDAP server, you can browse for an eDirectory User object. The information returned from eDirectory uses the following format:

cn=username,ou=orgunit,o=organization

If you are using another LDAP server, you must type the information in the format used by that LDAP server.

If the LDAP username for the POA requires a password, click Set Password, type the password twice for verification, then click Set Password.

For more information about LDAP usernames, see "Authenticating to GroupWise with Passwords Stored in an LDAP Directory" on page 1047.

6 If you want to prevent GroupWise users from changing their LDAP passwords by using the Password dialog box in the GroupWise client, select Disable LDAP Password Changing.

This option is deselected by default, so that if users change their passwords in the GroupWise client through the Security Options dialog box (GroupWise Windows client > Tools menu > Options > Security) or on the Passwords page (GroupWise WebAccess client > Options > Password), their LDAP passwords are changed to match the new passwords provided in the GroupWise client.

7 If the LDAP server is configured for bind connections, as described in "Providing LDAP Server Configuration Information" on page 461, specify the number of seconds the POA should maintain an inactive connection to the LDAP server.

The default is 30 seconds.

8 If you have only one LDAP server, click OK to save the security settings for the post office. You have provided all the necessary information to provide LDAP authentication for users in the post office.

or

If you have multiple LDAP servers and want to configure them into an LDAP server pool, click Apply, then continue with "Configuring a Pool of LDAP Servers" on page 464.

or

If you have multiple LDAP servers and want to configure them for failover, click OK to save the security settings for the post office, then continue with "Specifying Failover LDAP Servers (Non-SSL Only)" on page 465

Corresponding Startup Switches
You could also use the /ldapuser, /ldappwd, /ldapdisablepwdchg, and /ldaptimeout startup switches in the POA startup file to configure POA access to the LDAP server.

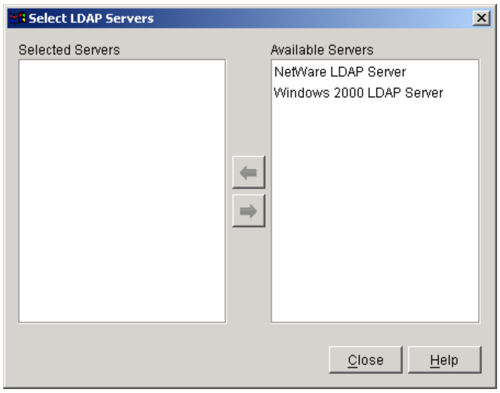
POA Web Console
You can see if LDAP is enabled on the Configuration page. Under the General Settings heading, click LDAP Authentication to view LDAP settings and change some of them for the current POA session.

Configuring a Pool of LDAP Servers

You can configure the POA to contact a different LDAP server each time it needs to access the LDAP directory. This provides load balancing and fault tolerance because each LDAP server in the pool is contacted equally often by the POA. The LDAP server pool can include as many as five servers.

1. Make sure you have enabled LDAP Authentication as described in "Enabling LDAP Authentication for a Post Office" on page 462.
2. In the LDAP Pool Server Reset Timeout field, specify the number of minutes the POA should wait before trying to contact an LDAP server in the pool that failed to respond to the previous contact.

   The default is 5 minutes.
3. Click Select Servers to define the specific pool of LDAP servers that you want to be available to users in this post office for LDAP authentication.



4. Select one or more LDAP servers in the Available Servers list, then click the arrow button to move them into the Selected Servers list.
5. Click OK to save the list of LDAP servers.
6. Click OK to save the security settings for the post office.

   ConsoleOne then notifies the POA to restart so the new LDAP settings can be put into effect.

Corresponding Startup Switches

You could also use the /ldapippool*n* and /ldappoolresettime startup switches in the POA startup file to configure the LDAP server pool and the timeout interval. If you choose to configure the LDAP server pool in the startup file rather than in ConsoleOne, additional switches must be provided to complete the configuration (/ldapportpool*n*, /ldapsslpool*n*, and /ldapsslkeypool*n*. Configuring the pool in ConsoleOne is the recommended approach.

If you previously set up LDAP authentication on the post office Security page in ConsoleOne and then you add the pooling startup switches to the POA startup file, the pooling switches override any LDAP information provided in ConsoleOne.

Specifying Failover LDAP Servers (Non-SSL Only)

If the POA does not need to use an SSL connection to your LDAP servers, you can use the /ldapipaddr switch to list multiple LDAP servers. Then, if the primary LDAP server fails to respond, the POA tries the next LDAP server in the list, and so on until it is able to access the LDAP directory. This provides failover LDAP servers for the primary LDAP server but does not provide load balancing, because the primary LDAP server is always contacted first.

1. Make sure you have provided the basic LDAP information on the post office Security page in ConsoleOne, as described in "Enabling LDAP Authentication for a Post Office" on page 462.
2. Edit the POA startup file with an ASCII text editor.

   For information about the POA startup file, see "Starting the POA" on page 431.
3. Use the /ldapipaddr startup switch to list addresses for multiple LDAP servers. Use a space between addresses.

   For example:

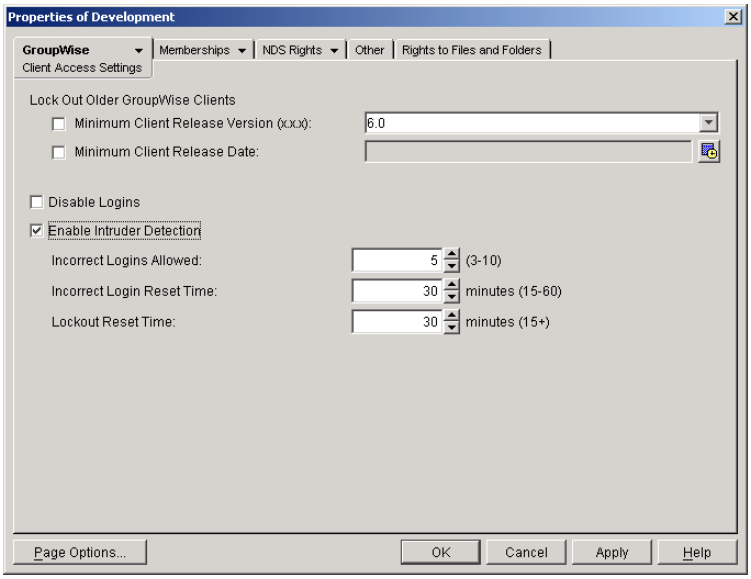
   /ldapipaddr-123.45.67.89 135.246.7.8 987.65.43.21

   IMPORTANT: Do not include any LDAP servers that require an SSL connection. There is currently no way to specify multiple SSL key files unless you are using pooled LDAP servers, as described in "Configuring a Pool of LDAP Servers" on page 464.
4. Save the POA startup file, then exit the text editor.
5. Stop the POA, then start the POA so that it reads the updated startup file.

Enabling Intruder Detection

You can configure the POA to detect system break-in attempts in the form of repeated unsuccessful logins. This feature can be especially helpful when allowing Remote client users to establish client/server connections to MTAs in your system. See "Enabling Live Remote" on page 589.

1. In ConsoleOne, browse to and right-click the Post Office object, then click Properties.
2. Click GroupWise > Client Access Settings to display the Client Access Settings page.



Lock Out Older GroupWise Clients

□ Minimum Client Release Version (x.x.x): 6.0

□ Minimum Client Release Date:

□ Disable Logins

☑ Enable Intruder Detection

Incorrect Logins Allowed: 5 (3-10)

Incorrect Login Reset Time: 30 minutes (15-60)

Lockout Reset Time: 30 minutes (15+)

3 Select Enable Intruder Detection.

4 Specify how many unsuccessful login attempts are allowed before the user is locked out.

The default is 5: valid values range from 3 to 10.

5 Specify in minutes how long unsuccessful login attempts are counted.

The default is 15; valid values range from 15 to 60.

6 Specify in minutes how long the user login is disabled.

The default is 30; the minimum setting is 15.

7 Click OK to save the intruder detection settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

If a user gets locked out by intruder detection, his or her GroupWise account is disabled. To restore access for the user in ConsoleOne, right-click the User object, click GroupWise > Account, then deselect Disable Logins. At restore access for the user at the POA Web console, click Configuration > Intruder Detection, then clear the lockout.

Corresponding Startup Switches

You could also use the /intruderlockout, /incorrectloginattempts, /attemptsresetinterval, and /lockoutresetinterval startup switches in the POA startup file to configure the POA for intruder detection.

POA Web Console

You can view current intruder detection settings on the Configuration page and change them using the Intruder Detection link.

Configuring Trusted Application Support

For background information about setting up trusted applications in ConsoleOne, see "Trusted Applications" on page 62.

Configuring Post Office Maintenance

You can configure the POA to manage databases and disk space in the post office on a regular basis:

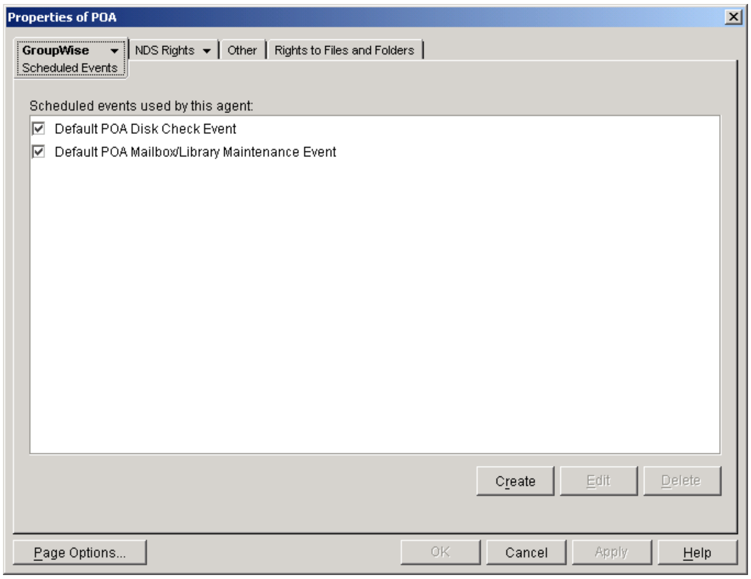
- "Scheduling Database Maintenance" on page 467
- "Scheduling Disk Space Management" on page 469
- "Performing Nightly User Upkeep" on page 472

Scheduling Database Maintenance

By default, the POA performs one recurring database maintenance event. At 12:00 a.m. each Friday, the POA performs a structural check of all user, message, and document databases in the post office. You can modify this default database maintenance event, or create additional database maintenance events for the POA to perform on a regular basis.

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Scheduled Events to display the Scheduled Events page.



Scheduled events used by this agent:

☑ Default POA Disk Check Event

☑ Default POA Mailbox/Library Maintenance Event

The Scheduled Events page lists a pool of POA events available to all POAs in your GroupWise system.

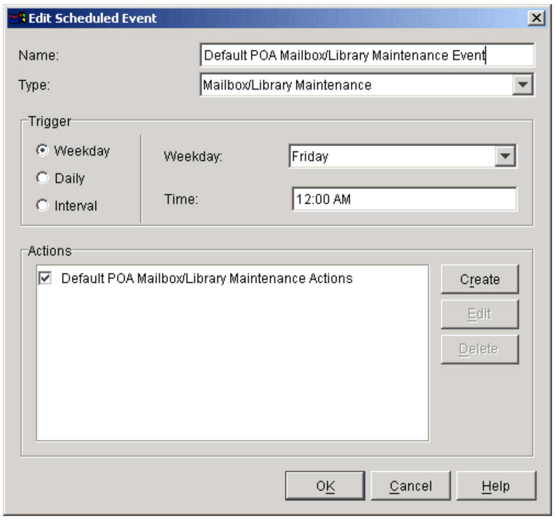
3 To modify the default database maintenance event, which would affect all POAs that have this database maintenance event enabled, select Default POA Mailbox/Library Maintenance Event, then click Edit.

or

To create a new database maintenance event, which will be added to the pool of POA events that can be enabled for any POA in your GroupWise system, click Create, then type a name for the new database maintenance event. Select Mailbox/Library Maintenance in the Type field.

NOTE: If the Create button is dimmed and you have a View button rather than an Edit button, you are connected to a secondary domain in a GroupWise system where Restrict System Operations to Primary

Domain has been selected under System Preferences. For more information, see "System Preferences" on page 44.



Edit Scheduled Event

Name: Default POA Mailbox/Library Maintenance Event

Type: Mailbox/Library Maintenance

Trigger

● Weekday
○ Daily
○ Interval

Weekday: Friday

Time: 12:00 AM

Actions

☑ Default POA Mailbox/Library Maintenance Actions

4 In the Trigger box, specify when you want the database maintenance event to take place.

You can have the database maintenance event take place once a week, once a day, or at any other regular interval, at whatever time you choose.

Below the Trigger box is listed the pool of POA database maintenance actions that are available for inclusion in all POA database maintenance events in your GroupWise system.

5 To modify the default database maintenance action, select Default POA Mailbox/Library Maintenance Actions, then click Edit.

or

To create a new database maintenance action, click Create, then type a name for the new database maintenance action.

Database maintenance actions and options you could schedule include:

Actions	Options on Actions
Analyze/Fix Databases	**Databases**
Structure	User
Index check	Message
Contents	Document
Collect statistics	**Logging**
Fix problems	Log file
Reset user disk space totals	Verbose log level
Analyze/Fix Library	**Results mailed to**
Verify library	Administrator
Fix document/version/element	Individual users
Verify document files	
Validate security	**Exclude**
Synchronize username	Selected users
Reassign orphaned documents	**Notification**
Reset word lists	Action status

For more detailed descriptions of the above actions, click Help in the Scheduled Event Actions dialog box. See also Chapter 27, "Maintaining User/Resource and Message Databases," on page 353 and Chapter 28, "Maintaining Library Databases and Documents," on page 359.

6 Select and configure the database maintenance action to perform for the database maintenance event.

7 Click OK three times to close the various scheduled event dialog boxes and save the modified database maintenance event.

ConsoleOne then notifies the POA to restart so the new or modified database maintenance event can be put into effect.

POA Web Console

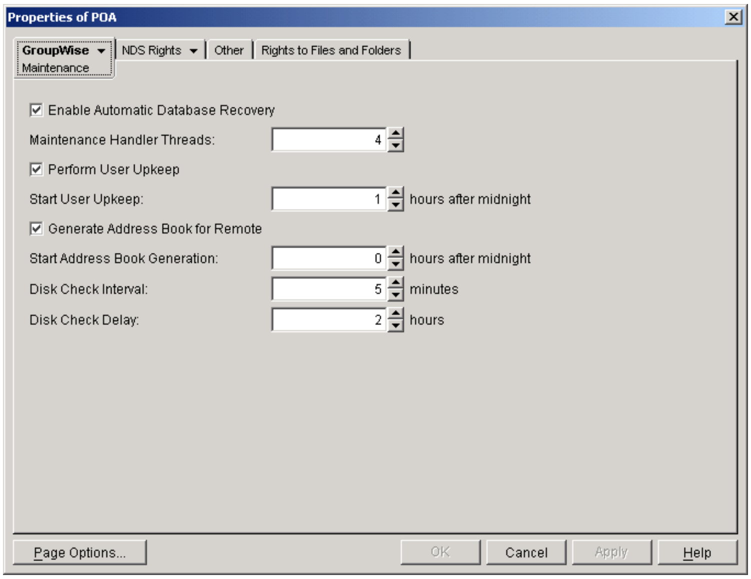
You can see what database maintenance events the POA is scheduled to perform at the bottom of the Configuration page.

Scheduling Disk Space Management

By default, the POA performs one recurring disk space management event. Every 5 minutes, the POA checks to make sure there is at least 100 MB of free disk space in the post office directory. If there is ever less than 100 MB of free disk space, the POA performs a Reduce operation on the user and message databases in the post office. You can modify this default disk space management event, or create additional disk space management events for the POA to perform on a regular basis.

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Maintenance to display the POA Maintenance page.



☑ Enable Automatic Database Recovery

Maintenance Handler Threads: 4

☑ Perform User Upkeep

Start User Upkeep: 1 hours after midnight

☑ Generate Address Book for Remote

Start Address Book Generation: 0 hours after midnight

Disk Check Interval: 5 minutes

Disk Check Delay: 2 hours

3 To change the interval at which the selected POA checks for free disk space in its post office, adjust the number of minutes in the Disk Check Interval field as needed.

The default is 5 minutes, which could be much too frequent if plenty of disk space is readily available.

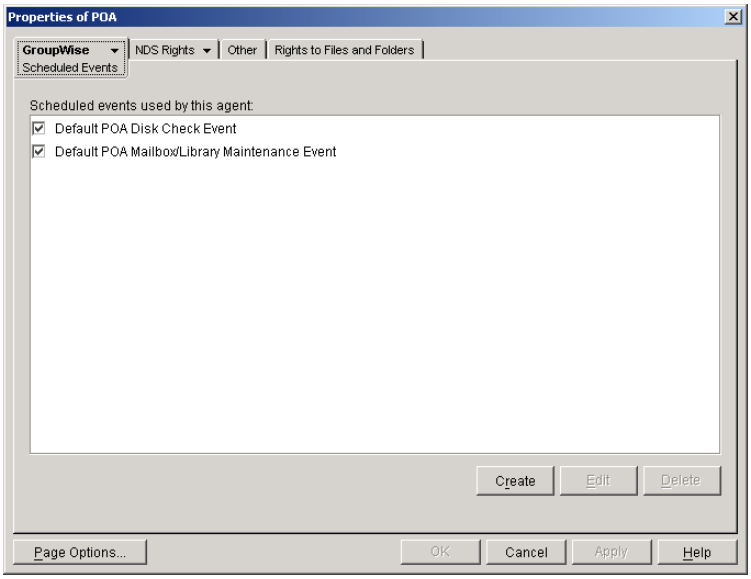
When a disk space problem is encountered, the time interval no longer applies until after the situation has been corrected. Instead, the POA continually checks available disk space to determine if it can restart message threads that have been suspended because of the low disk space condition.

4 To change the amount of time the POA allows to pass before notifying the administrator again of an already reported problem condition, adjust the number of hours in the Disk Check Delay field as needed.

The default is 2 hours.

5 Client Apply to save the maintenance settings.

6 Click GroupWise > Scheduled Events to display the Scheduled Events page.



Scheduled events used by this agent:

☑ Default POA Disk Check Event

☑ Default POA Mailbox/Library Maintenance Event

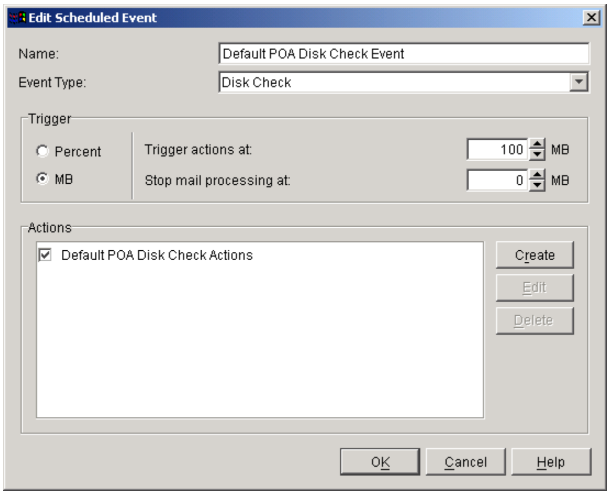
The Scheduled Events page lists a pool of POA events available to all POAs in your GroupWise system.

7 To modify the default disk space management event, which would affect all POAs that have this disk space management event enabled, select Default POA Disk Check Event, then click Edit.

or

To create a new disk space management event, which will be added to the pool of POA events that can be enabled for any POA in your GroupWise system, click Create, then type a name for the new disk space management event. Select Disk Check in the Type field.

NOTE: If the Create button is dimmed and you have a View button rather than an Edit button, you are connected to a secondary domain in a GroupWise system where Restrict System Operations to Primary Domain has been selected under System Preferences. For more information, see "System Preferences" on page 44.



Edit Scheduled Event

Name: Default POA Disk Check Event

Event Type: Disk Check

Trigger

○ Percent

● MB

Trigger actions at: 100 MB

Stop mail processing at: 0 MB

Actions

☑ Default POA Disk Check Actions

8 In the Trigger box, select Percent or MB to determine whether you want the amount of available disk space measured by percentage or by megabytes.

9 In the Trigger Actions At field, specify the minimum amount of available disk space you want to have in the post office. When the minimum amount is reached, the Disk Check actions are triggered

10 In the Stop Mail Processing At field, specify the minimum amount of available disk space at which you want the POA to stop receiving and processing messages.

Below the Trigger box is listed the pool of disk space management actions that are available for inclusion in all POA disk space management events in your GroupWise system.

11 To modify the action that the default disk space management event includes, select Default POA Disk Check Actions, then click Edit.

or

To create a new disk space management action, click Create, then type a name for the new disk space management action.

Disk space management actions and options you could schedule include:

Actions	Options on Actions
Reduce/Expire Messages Reduce only Expire and reduce - Items older than - Downloaded items older than - Items larger than - Trash older than - Reduce mailbox to - Reduce mailbox to limited size Include - Received items - Sent items - Calendar items - Only backed-up items **Archive/Delete Documents** **Delete Activity Logs**	**Databases** User Message Document **Logging** Log file Verbose log level **Results** Administrator Individual users **Misc** Support options **Exclude** Selected users

For more detailed descriptions of the above actions, click Help in the Scheduled Event Actions dialog box. See also Chapter 30, "Managing Database Disk Space," on page 367.

12 Select and configure the disk space management action to perform.

13 Click OK twice to close the scheduled event dialog boxes and save the modified disk space management event.

ConsoleOne then notifies the POA to restart so the new or modified disk space management event can be put into effect.

You might want to create several disk space management events with different triggers and actions. For example, at 250 MB, you could mail a warning to the administrator; at 200 MB, you could have the POA perform a Reduce Only; at 150 MB, you could have the POA perform an Expire and Reduce.

For some specific suggestions on implementing disk space management, see "Managing Disk Space Usage in the Post Office" on page 171.

POA Web Console
You can view the currently scheduled disk check events on the Scheduled Events page.

Performing Nightly User Upkeep

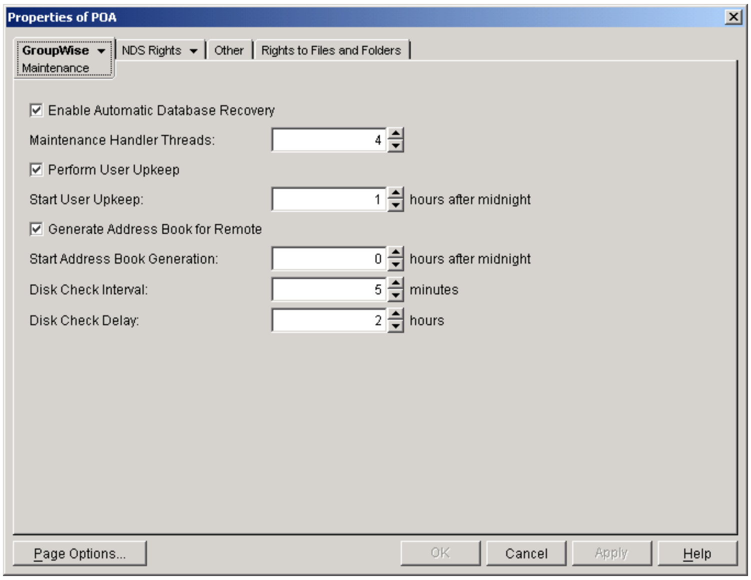
To keep GroupWise users' mailboxes and calendars up to date, the following activities must be performed each day:

- Delete expired items from users' mailboxes
- Empty expired items from the Trash
- Synchronize each user's Frequent Contacts Address Book with the system Address Book
- Advance uncompleted tasks to the next day
- Generate a current copy of the system Address Book for Remote and Caching users

The first two activities used to be performed by the GroupWise client, but to minimize user wait time, the client no longer deletes expired items. The last two activities can still be performed by the GroupWise client when needed, but the required processing might cause users to wait. You can configure the POA to take care of these user upkeep activities once a day, at a convenient time.

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Maintenance to display the POA Maintenance page.



☑ Enable Automatic Database Recovery

Maintenance Handler Threads: 4

☑ Perform User Upkeep

Start User Upkeep: 1 hours after midnight

☑ Generate Address Book for Remote

Start Address Book Generation: 0 hours after midnight

Disk Check Interval: 5 minutes

Disk Check Delay: 2 hours

3 Select Perform User Upkeep.

4 In the Start User Upkeep field, specify the number of hours after midnight for the POA to start performing user upkeep.

The default is 1 hour.

5 If you have Remote or Caching users, select Generate Address Book for Remote.

6 Specify the number of hours after midnight for the POA to generate the daily copy of the system Address Book for Remote and Caching users.

The default is 0 hours (that is, at midnight).

If you want to generate the system Address Book for download more often than once a day, you can delete the existing wprof50.db file from the \wpcsout\ofs subdirectory of the post office. A new downloadable system Address Book will be automatically generated for users in the post office.

7 Click OK to save the new nightly user maintenance settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches

You could also configure nightly user upkeep using startup switches in the POA startup file. By default, nightly user upkeep is enabled. Use the /nuuoffset and /rdaboffset switches to specify the start times.

POA Web Console

You can view the current user upkeep schedule on the Scheduled Events page.

38 Monitoring the POA

By monitoring the POA, you can determine whether or not its current configuration is meeting the needs of the post office it services. You have a variety of tools to help you monitor the operation of the POA:

- "Using the POA Agent Console" on page 475
- "Using the POA Web Console" on page 489
- "Using POA Log Files" on page 497
- "Using GroupWise Monitor" on page 498
- "Using NetWare 6.5 Remote Manager" on page 498
- "Using SNMP Monitoring Programs" on page 499
- "Notifying the GroupWise Administrator" on page 503
- "Using the POA Error Message Documentation" on page 504
- "Employing POA Troubleshooting Techniques" on page 504
- "Using Platform-Specific POA Monitoring Tools" on page 505

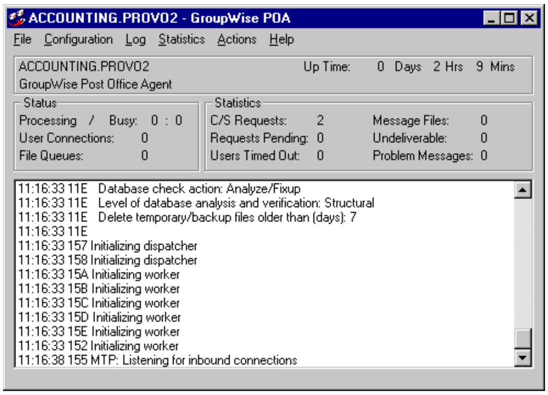
Using the POA Agent Console

The following topics help you monitor and control the POA from the POA agent console:

- "Monitoring the POA from the POA Agent Console" on page 475
- "Controlling the POA from the POA Agent Console" on page 479

Monitoring the POA from the POA Agent Console

The POA agent console provides information, status, and message statistics about the POA to help you assess its current functioning.



ACCOUNTING.PROVO2 Up Time: 0 Days 2 Hrs 9 Mins
GroupWise Post Office Agent

Status
Processing / Busy: 0 : 0
User Connections: 0
File Queues: 0

Statistics
C/S Requests: 2
Requests Pending: 0
Users Timed Out: 0
Message Files: 0
Undeliverable: 0
Problem Messages: 0

```
11:16:33 11E   Database check action: Analyze/Fixup
11:16:33 11E   Level of database analysis and verification: Structural
11:16:33 11E   Delete temporary/backup files older than (days): 7
11:16:33 11E
11:16:33 157 Initializing dispatcher
11:16:33 158 Initializing dispatcher
11:16:33 15A Initializing worker
11:16:33 15B Initializing worker
11:16:33 15C Initializing worker
11:16:33 15D Initializing worker
11:16:33 15E Initializing worker
11:16:33 152 Initializing worker
11:16:38 155 MTP: Listening for inbound connections
```

Linux Note: You must use the --show startup switch in order to display the Linux POA agent console. See "Starting the Linux POA" on page 433

Windows Note: You can suppress the Windows POA agent console by running the POA as a service. See "Starting the Windows POA" on page 434.

The POA agent console consists of several components:

- "POA Information Box" on page 476
- "POA Status Box" on page 476
- "POA Statistics Box" on page 477
- "POA Log Message Box" on page 478
- "POA Admin Thread Status Box" on page 478

Do not exit the POA agent console unless you want to stop the POA.

NetWare Note: At a NetWare® server console, you can use Alt+Esc to change screens. In a remote console window, you can use Alt+F1 to select a screen to view. You can use these keystrokes to display the POA agent console if it is not immediately visible on the NetWare console.

Linux Note: On a Linux server, you can minimize the POA agent console, but do not close it unless you want to stop the POA.

Windows Note: On a Windows server, you can minimize the POA agent console, but do not close it unless you want to stop the POA.

POA Information Box

The POA Information box identifies the POA whose POA agent console you are viewing, which is especially helpful when multiple POAs are running on the same server.

PostOffice.Domain: Displays the name of the post office serviced by this POA, and what domain it is linked to.

Description: Displays the description provided in the Description field in the POA Identification page in ConsoleOne. When you run multiple POAs on the same server, the description should uniquely identify each one. If multiple administrators work at the server where the POA runs, the description could include a note about who to contact before stopping the POA.

Up Time: Displays the length of time the POA has been running.

POA Web Console
The Status page also displays this information.

POA Status Box

The POA Status box displays the current status of the POA and its backlog. The information displayed varies depending on whether the POA is processing client/server connections, message files, both, or neither.

Processing: Displays a rotating bar when the POA is running. If the bar is not rotating, the POA has stopped. For assistance, see "Post Office Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Busy: Displays the number of POA threads currently in use (busy) for client/server connections, message files, or both, depending on POA configuration. You can change the total number of threads available. See "Adjusting the Number of Connections for Client/Server Processing" on page 508 and "Adjusting the Number of POA Threads for Message File Processing" on page 512.

User Connections (for client/server processing): Displays the number of active application ("virtual") TCP/IP connections between the POA and the GroupWise® clients run by GroupWise users. You can change the maximum number of user connections. See "Adjusting the Number of Connections for Client/Server Processing" on page 508.

Physical Connections (for client/server processing): Displays the number of active physical TCP/IP connections between the post office and the GroupWise clients run by GroupWise users. You can change the maximum number of physical connections. See "Adjusting the Number of Connections for Client/Server Processing" on page 508.

Priority Queues (for message file processing): Displays the number of messages waiting in the high priority message queues. You can control the number of threads processing message files. See "Adjusting the Number of POA Threads for Message File Processing" on page 512.

Normal Queues (for message file processing): Displays the number of messages waiting in the normal priority message queues. You can control the number of threads processing message files. See "Adjusting the Number of POA Threads for Message File Processing" on page 512.

File Queues (for message file processing): Displays the total number of messages waiting in all message queues, when client/server information and message file information are displayed together.

The number of messages displayed as waiting in message queues is not an exact count. For example, if the POA detects numerous messages to process in the priority 4 queue (normal messages), it does not scan and count messages in lower priority queues. Therefore, actual counts of message files waiting in queues could be higher than the counts displayed in the Status box.

For information about the various message queues in the post office, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

POA Web Console
The Status page also displays the status information listed above. In addition, you can display detailed information about specific queue contents.

POA Statistics Box

The POA Statistics box displays statistics showing the current workload of the POA. The information displayed varies depending on whether the POA is processing client/server connections, message files, both, or neither.

C/S Requests (for client/server processing): Displays the number of active client/server requests between GroupWise clients and the POA.

Requests Pending (for client/server processing): Displays the number of client/server requests from GroupWise clients the POA has not yet been able to respond to. If the number is large, see "POA Statistics Box Shows Requests Pending" in "Post Office Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Users Timed Out (for client/server processing): Displays the number of GroupWise clients no longer communicating with the POA. If the number is large, see "POA Statistics Box Shows Users Timed Out" in "Post Office Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Message Files (for message file processing): Displays the total number of messages processed by the POA. This includes user messages, status messages, and service requests processed by the POA.

Undeliverable (for message file processing): Displays the number of messages that could not be delivered because the user was not found in that post office or because of other similar problems. Senders of undeliverable messages are notified. For assistance, see "Message Has Undeliverable Status" in "Strategies for Message Delivery Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Problem Messages (for message file processing): Displays the number of invalid message files that have problems not related to user error. It also displays requests the POA cannot process because of error conditions. For assistance, see "Message Is Dropped in the problem Directory" in "Strategies for Message Delivery Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Users Delivered: Displays the number of user messages delivered to recipients in the post office. A message with six recipients in the local post office is counted six times.

Statuses: Displays the number of status messages delivered to recipients in the post office.

Rules Executed: Displays the number of users' rules executed by the POA.

POA Web Console
The Status page also displays this information. In addition, you can display detailed information about client/server connections and message file processing.

POA Log Message Box

The POA Log Message box displays the same information that is being written to the POA log file. The amount of information displayed in the POA Log Message box depends on the current log settings for the POA. See "Using POA Log Files" on page 497. The information scrolls up automatically.

Windows Note: To stop the automatic scrolling, click Log, then deselect Auto Scroll.You can then use the scroll bar to browse through the contents of the log message box.

POA Web Console
You can view and search POA log files on the Log Files page.

Informational Messages

When you first start the POA, you typically see informational messages that list current agent settings, current number of threads, TCP/IP options (client/server), and scheduled events. As the POA runs, it continues to provide status and delivery information in the POA Log Message box.

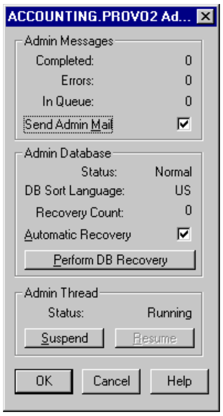
Error Messages

If the POA encounters a problem processing a message, it displays an error message in the POA Log Message box. See "Post Office Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

POA Admin Thread Status Box

The POA admin thread updates the post office database (wphost.db) when users and/or user information are added, modified, or removed, and repairs it when damage is detected.

To display the POA Admin Thread Status box from the POA agent console, click Configuration > Admin Status.



ACCOUNTING.PROVO2 Ad...

Admin Messages

Completed: 0

Errors: 0

In Queue: 0

Send Admin Mail ☑

Admin Database

Status: Normal

DB Sort Language: US

Recovery Count: 0

Automatic Recovery ☑

Admin Thread

Status: Running

The following tasks pertain specifically to the POA admin thread:

- "Suspending/Resuming the POA Admin Thread" on page 481
- "Displaying POA Admin Thread Status" on page 484
- "Recovering the Post Office Database Automatically or Immediately" on page 485

POA Web Console

You can display POA admin thread status on the Configuration page. Under the General Settings heading, click Admin Task Processing. You can also change the admin settings for the current POA session.

Controlling the POA from the POA Agent Console

You can perform the following tasks to monitor and control the POA from the POA agent console at the server where the POA is running:

- "Stopping the POA" on page 480
- "Suspending/Resuming the POA Admin Thread" on page 481
- "Displaying the POA Software Date" on page 481
- "Displaying Current POA Settings" on page 481
- "Displaying Detailed Statistics about POA Functioning" on page 482
- "Displaying Client/Server Information" on page 482
- "Listing Message Queue Activity" on page 483
- "Displaying Message Transfer Status" on page 483
- "Restarting the MTP Thread" on page 484
- "Displaying POA Admin Thread Status" on page 484
- "Recovering the Post Office Database Automatically or Immediately" on page 485
- "Recovering User and Message Databases Automatically" on page 486
- "Updating QuickFinder Indexes" on page 486
- "Compressing QuickFinder Indexes" on page 487
- "Browsing the Current POA Log File" on page 487

- "Viewing a Selected POA Log File" on page 488
- "Cycling the POA Log File" on page 488
- "Adjusting POA Log Settings" on page 488
- "Editing the POA Startup File" on page 489
- "Accessing Online Help for the POA" on page 489

Stopping the POA

You might need to stop and restart the POA for the following reasons:

- Updating the agent software
- Troubleshooting message flow problems
- Backing up GroupWise databases
- Rebuilding GroupWise databases

To stop the POA from the POA agent console:

1 Click File > Exit > Yes.

NetWare Note: Use Exit (F7). If the POA does not respond to Exit, you can use the unload command to stop the POA. However, this would stop all instances of the POA running on the server.

Linux Note: If the Linux POA does not respond to Exit, you can kill the POA process, as described below, but include the -9 option.

Windows Note: If the Windows POA does not respond to Exit, you can close the POA agent console to stop the POA or use the Task Manager to terminate the POA task.

2 Restart the POA. See "Starting the POA" on page 431.

To stop the POA on Linux when it is running in the background as a daemon:

1 Make sure you are logged in as root.

2 If you started the Linux POA using the grpwise script:

2a Change to the /etc/init.d directory.

2b Enter the following command:

```
./grpwise stop
```

2c Skip to Step 4

3 If you started the Linux POA manually (not using the grpwise script):

3a Determine the process IDs (PIDs) of the POA:

```
ps -eaf | grep gwpoa
```

The PIDs for all gwpoa processes are listed.

You can also obtain this information from the Environment page of the POA Web console.

3b Kill the first POA process listed:

Syntax:

```
kill PID
```

Example:

```
kill 1483
```

It might take a few seconds for all POA processes to terminate.

4 Use the ps command to verify that the POA has stopped.

```
ps -eaf | grep gwpoa
```

Suspending/Resuming the POA Admin Thread

You can cause the POA to stop accessing the post office database (wphost.db) without stopping the POA completely. For example, you could suspend the POA admin thread while backing up the post office database.

To suspend the POA admin thread:

1 At the POA agent console, click Configuration > Admin Status.

2 Click Suspend.

NetWare Note: Use Options (F10) > Admin Status > Suspend.

The POA admin thread no longer accesses the post office database until you resume processing.

To resume the POA admin thread:

1 At the POA agent console, click Configuration > Admin Status.

2 Click Resume.

NetWare Note: Use Options (F10) > Admin Status > Resume.

POA Web Console
You can suspend and resume the POA admin thread from the Configuration page. Under the General Settings heading, click Admin Task Processing > Suspend or Resume > Submit.

Displaying the POA Software Date

It is important to keep the POA software up-to-date. You can display the date of the POA software from the POA agent console.

1 At the server where the POA is running, display the POA agent console.

2 Click Help > About POA.

NetWare Note: To check the date of the POA NetWare®, you must list the gwpoa.nlm file in the agent installation directory (typically, in the sys:\system directory) or use the `modules gwpoa.nlm` command at the server console prompt.

POA Web Console
You also check the POA software date on the Environment page.

Displaying Current POA Settings

You can list the current configuration settings of the POA at the POA agent console.

1 At the server where the POA is running, display the POA agent console.

2 Click Configuration > Agent Settings.

The configuration information displays in the log message box and is written to the log file.

NetWare Note: Use Show Configuration (F4) > Show Configuration.

If information you need scrolls out of the log message box, you can scroll back to it. See "Browsing the Current POA Log File" on page 487.

For information about POA configuration settings, see Chapter 37, "Configuring the POA," on page 437 and Chapter 40, "Using POA Startup Switches," on page 523.

POA Web Console
You check the current POA settings on the Configuration page.

Displaying Detailed Statistics about POA Functioning

The POA agent console displays essential information about the functioning of the POA. More detailed information is also available.

1 At the server where the POA is running, display the POA agent console.

2 Click Statistics > Misc. Statistics.

NetWare Note: This feature is not available in the NetWare POA.

3 Review the Detailed Statistics dialog box. The following statistics are displayed and written to the log file for the current POA up time:

- Databases rebuilt
- Users deleted
- Users moved
- Moved messages processed
- Statuses processed

POA Web Console
You can display statistics on the Status page.

Displaying Client/Server Information

When the POA and the GroupWise clients communicate in client/server mode, you can display statistics to indicate the performance level of the TCP/IP communication.

1 At the server where the POA is running, display the POA agent console.

2 Click Statistics > Client/Server.

NetWare Note: Use Configuration (F4) > Display Client/Server Information.

3 Click the type of statistics to display.

The selected type of statistics for the current POA up time are listed in the message log box and are written to the POA log file.

If information you need scrolls out of the log message box, you can scroll back to it. See "Browsing the Current POA Log File" on page 487.

All Statistics: Lists the information for General Statistics, Throughput, Physical Connections, and Application Connections, as described below.

General Statistics: Lists the DNS address and IP address of the server, along with the TCP port for the POA, the number of messages received, sent, and aborted, and the number of physical and application connections active and allowed.

Show Throughput: Lists the total number of messages processed by the POA for all users. Statistics are provided for the current elapsed time and as a per second average.

Clear Throughput: Resets the current elapsed time to zero.

Physical Connections: Lists the currently active physical connections. Physical connections are active TCP connections created whenever GroupWise users do something that requires communication and closed when the specific activities have been completed. By listing the physical connections, you can see what users are actively using GroupWise and how much throughput each user is generating. Users' IP addresses are also listed.

Application Connections: Lists the currently active application connections. Every user that starts GroupWise has an application connection for as long as GroupWise is running, even if GroupWise is not actively in use at the moment. By listing the application connections, you can see what users have started GroupWise and how much throughput each user is generating. Users' IP addresses are also listed.

Show Redirection List: Lists all POAs in your GroupWise system and indicates whether each is configured for TCP/IP. The list includes the IP address of each POA and the IP address of its proxy server outside the firewall, if applicable. This redirection information is obtained from the post office database (wphost.db).

Check Redirection List: Attempts to contact each POA in your GroupWise system and reports the results. If a POA is listed as "Connection Failed," see "Post Office Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

POA Web Console

You can display client/server information on the Configuration page. You can list client/server users from the Status page using the C/S Users and Remote/Caching Users links.

Listing Message Queue Activity

The POA uses eight queues to process message files. You can view the activity in each of these queues. For more information about message queues, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

1. At the server where the POA is running, display the POA agent console.
2. Click Actions > View MF Queues.

   NetWare Note: Use Options (F10) > Actions > View MF Queues.
3. View the queue activity in the message log box. Use the scroll bar if necessary to scroll through the information.

   If information you need scrolls out of the log message box, you can scroll back to it. See "Browsing the Current POA Log File" on page 487.

   The information is also written to the POA log file.

You can check queue activity on the Status page. Under the Thread Status heading, click the type of thread to view queue activity for.

Displaying Message Transfer Status

When the POA links to the MTA by way of TCP/IP, you can view the status of the TCP/IP link from the POA agent console.

1. At the server where the POA is running, display the POA agent console.
2. Click Configuration > Message Transfer Status.

   NetWare Note: Use Options (F10) > Message Transfer Status.

3. View the following information about the TCP/IP link:

   Outbound TCP/IP Address: Displays the TCP/IP address and port where the MTA listens for messages from the POA.

   Inbound TCP/IP Address: Displays the TCP/IP address and port where the POA listens for messages from the MTA.

   Hold Directory: Displays the path to the directory where the POA stores messages if the TCP/IP link to the MTA is closed.

   Current Status: Lists the current status of the TCP/IP link.

   - **Open:** The POA and the MTA are successfully communicating by way of TCP/IP.
   - **Closed:** The POA is unable to contact the MTA by way of TCP/IP
   - **Unavailable:** The POA is not yet configured for TCP/IP communication with the MTA.
   - **Unknown:** The POA is unable to contact the MTA in any way.

   Messages Written: Displays the number of messages the POA has sent.

   Message Read: Displays the number of messages the POA has received.

   Last Closure Reason: Provides an explanation for why the post office was last closed. For assistance resolving closure reasons, see "Post Office Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

POA Web Console
You can display message transfer status on the MTP Status page.

Restarting the MTP Thread

When the POA links to the MTA by way of TCP/IP, you can restart the Message Transfer Protocol (MTP) thread that provides the link between the POA and the MTA.

1. At the server where the POA is running, display the POA agent console.
2. Click Actions > Restart MTP.

   NetWare Note: Use Options (F10) > Actions > Restart MTP.

POA Web Console
You can restart the MTA thread from the Configuration page. Click Message Transfer Protocol > Restart MTP > Submit. In addition, you can control the send and receive threads separately on the MTP Status page. In the Send or Receive column, click the current status > Stop/Start MTP Send/ Receive > Submit.

Displaying POA Admin Thread Status

Status information for the POA admin thread is displayed in a separate dialog box, rather than on the main POA agent console.

1. At the server where the POA is running, display the POA agent console.
2. Click Configuration > Admin Status.

   NetWare Note: Use Options (F10) > Admin Status.

   The following admin status information is displayed:

Admin Message Box
The Admin Message box provides the following information about the workload of the POA admin thread:

Completed: Number of administrative message successfully processed.

Errors: Number of administrative messages not processed because of errors.

In Queue: Number of administrative messages waiting in the queue to be processed.

Send Admin Mail: Select this options to send a message to the administrator whenever a critical error occurs. See "Notifying the GroupWise Administrator" on page 503.

Admin Database Box
The Admin Database box provides the following information about the post office database (wphost.db):

Status: Displays one of the following statuses:

- **Normal:** The POA admin thread is able to access the post office database normally.
- **Recovering:** The POA admin thread is recovering the post office database.
- **DB Error:** The POA admin thread has detected a critical database error. The post office database cannot be recovered. Rebuild the post office database in ConsoleOne. See "Rebuilding Domain or Post Office Databases" on page 349.

  The POA admin thread does not process any more administrative messages until the database status has returned to Normal.
- **Unknown:** The POA admin thread cannot determine the status of the post office database. Exit the POA, then restart it, checking for errors on startup.

DB Sort Language: Displays the language code for the language that determines the sort order of lists displayed in ConsoleOne and the GroupWise system Address Book.

Recovery Count: Displays the number of recoveries performed on the post office database by this POA for the current POA session.

Admin Thread Box
The Admin Thread box displays the following information:

Status: Displays one of the following statuses:

- **Running:** The POA admin thread is active.
- **Suspended:** The POA admin thread is not processing administrative messages.
- **Starting:** The POA admin thread is initializing.
- **Terminated:** The POA admin thread is not running.

POA Web Console
You can display POA admin thread status from the Configuration page. Under the General Settings heading, click Admin Task Processing.

Recovering the Post Office Database Automatically or Immediately

The POA admin thread can recover the post office database (wphost.db) when it detects a problem.

To enable/disable automatic post office database recovery:

1 At the server where the POA is running, display the POA agent console.

2. Click Configuration > Admin Status > Automatic Recovery to toggle this feature on or off for the current POA session.

   NetWare Note: Use Options (F10) > Admin Status > Automatic Recovery.

To change the setting permanently, see "Configuring the POA in ConsoleOne" on page 439.

To recover the post office database immediately:

1. At the server where the POA is running, display the POA agent console.
2. Click Configuration > Admin Status > Perform DB Recovery.

   NetWare Note: Use Options (F10) > Admin Status > Perform DB Recovery.

For additional database repair procedures, see Chapter 26, "Maintaining Domain and Post Office Databases," on page 345.

POA Web Console
You can recover the post office database from the Configuration page. Under the General Settings heading, click Admin Task Processing. Select Automatic Recovery or Perform DB Recovery as needed.

Recovering User and Message Databases Automatically

The POA can recover user databases (user*xxx*.db) and message databases (msg*nn*.db) automatically when it detects a problem because databases can be open during the recover process. This procedure is a "recover" rather than a "rebuild," because a "rebuild" requires that all users and agents be out of the database being rebuilt. See Chapter 27, "Maintaining User/Resource and Message Databases," on page 353.

To enable/disable automatic message and user database recovery:

1. At the server where the POA is running, display the POA agent console.
2. Click Actions > Auto Rebuild to toggle this feature on or off for the current POA session.

   NetWare Note: Use Options (F4) > Actions > Enable Auto Rebuild.

To change the setting permanently, see "Configuring the POA in ConsoleOne" on page 439.

POA Web Console
You can see whether automatic message and user database recovery is enabled on the Configuration page under the Performance Settings heading.

Updating QuickFinder Indexes

GroupWise uses QuickFinder® technology to index messages and documents stored in post offices. You can start indexing from the POA agent console. For example, if you just imported a large number of documents, you could start indexing immediately, rather than waiting for the next scheduled indexing cycle.

To update QuickFinder indexes for the post office:

1. At the server where the POA is running, display the POA agent console.
2. Click Actions > QuickFinder > Update Indexes.

   NetWare Note: Use Options (F10) > Actions > Update QuickFinder Indexes.

To avoid overloading the POA with indexing processing, a maximum of 1000 items are indexed per database. If a very large number of messages are received regularly, or if a user with a very large mailbox is moved to a different post office (requiring the user's messages to be added into the new post office indexes), you might need to repeat this action multiple times in order to get all messages indexed. If too many repetitions would be required to complete the indexing task, refer to TID10063970 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10063970.htm) for assistance.

You can set up indexing to occur at regular intervals. See "Regulating Indexing" on page 514.

If the indexing load on the POA is heavy, you can set up a separate POA just for indexing. See "Configuring a Dedicated Indexing POA" on page 516.

POA Web Console
You can update QuickFinder indexes from the Configuration page. Under the General Settings heading, click QuickFinder Indexing.

Compressing QuickFinder Indexes

QuickFinder indexes are automatically compressed at midnight each night to conserve disk space. You can start compression at any other time from the POA agent console. For example, if you just imported and indexed a large number of documents and are running low on disk space, you could compress the indexes immediately, rather than waiting for it to happen at midnight.

To compress QuickFinder indexes for the post office:

1. At the server where the POA is running, display the POA agent console.
2. Click Actions > QuickFinder > Compress Indexes.

   NetWare Note: Use Options (F10) > Actions > Compress QuickFinder Indexes.

POA Web Console
You can compress QuickFinder indexes from the Configuration page. Under the General Settings heading, click QuickFinder Indexing.

Browsing the Current POA Log File

In the log message box, the POA displays the same information being written to the POA log file. The amount of information depends on the current log settings for the POA.

The information automatically scrolls up the screen as additional information is written. You can stop the automatic scrolling so you can manually scroll back through earlier information.

To browse the current POA log file and control scrolling:

1. At the server where the POA is running, display the POA agent console.
2. Click Log > Auto Scroll to toggle automatic scrolling on or off.

   NetWare Note: Use View Log File (F9).

For explanations of messages in the POA log file, see "Post Office Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

See also "Using POA Log Files" on page 497.

POA Web Console
You can browse and search POA log files on the Log Files page.

Viewing a Selected POA Log File

Reviewing log files is an important way to monitor the functioning of the POA.

1. At the server where the POA is running, display the POA agent console.
2. Click Log > View Log.

   NetWare Note: Use Options (F10) > View Log Files.

   The following information is provided:

   Log Files: Lists the current POA log files, ordered from the oldest log file at the top to the newest log file at the bottom. The current log file is marked with an asterisk (*).

   Date/Time: Displays the date and time of each POA log file.

   Space Used: Displays the amount of disk space currently occupied by that POA's log files. You can control the amount of space consumed by POA log files during the current POA session. You can also control the default amount of disk space for POA log files in the POA Log Settings page in ConsoleOne or in the POA startup file. See "Configuring POA Log Settings and Switches" on page 497.

   Log File Directory: Displays the full path of the directory where the POA writes its log files. See "Configuring POA Log Settings and Switches" on page 497.
3. In the log file list, select the POA log file you want to view.

   Windows Note: For the Windows POA, you can select the viewer to use by providing the full path to the viewer program. The default viewer is Notepad.
4. Click View.

For explanations of messages in the POA log file, see "Post Office Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

See also "Using POA Log Files" on page 497.

POA Web Console
You can view and search POA log files on the Log Files page.

Cycling the POA Log File

You can have the POA start a new log file as needed.

1. At the server where the POA is running, display the POA agent console.
2. Click Log > Cycle Log.

   NetWare Note: Use Options (F10) > Cycle Log.

Adjusting POA Log Settings

Default log settings are established when you start the POA. However, you can adjust the POA log settings for the current session from the POA agent console. This overrides any settings provided in ConsoleOne or in the POA startup file. The modified settings remain in effect until you restart the POA, at which time the log settings specified in ConsoleOne or the startup file take effect again.

1. At the server where the POA is running, display the POA agent console.
2. Click Log > Log Settings.

   NetWare Note: Use Options (F10) > Logging Options.

3. Adjust the values as needed for the current POA session.

   See "Using POA Log Files" on page 497.

POA Web Console
You can adjust POA log settings from the Configuration page. Click the Log Settings heading.

Editing the POA Startup File

You can change the configuration of the POA by editing the POA startup file from the POA agent console.

1. At the server where the POA is running, display the POA agent console.
2. Click Configuration > Edit Startup File.

   NetWare Note: Use Options (F10) > Actions > Edit Startup File.
3. Make the necessary changes, then save and exit the startup file.
4. Stop and restart the POA.

Accessing Online Help for the POA

Click Help on the menu bar for information about the POA agent console. Click the Help button in any dialog box for additional information.

NetWare Note: Press F1 for information in any dialog box or menu.

Using the POA Web Console

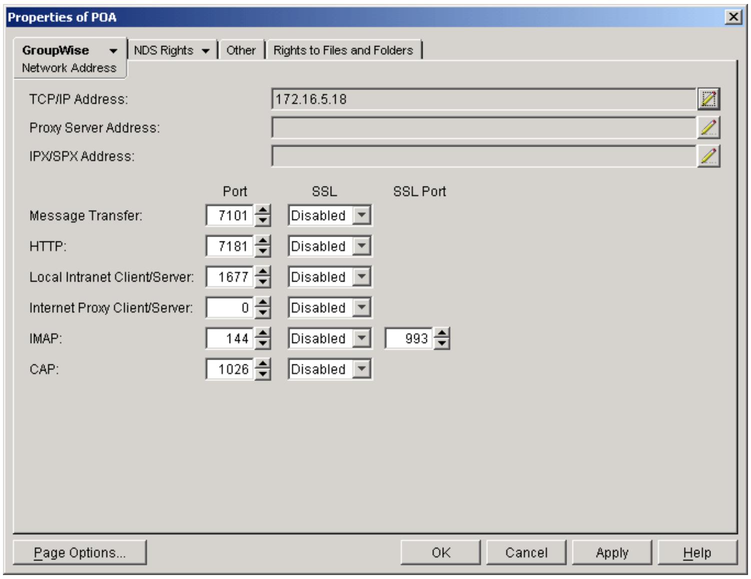
The POA Web console enables you to monitor and control the POA from any location where you have access to a Web browser and the Internet. This provides substantially more flexible access than the POA agent console, which can only be accessed from the server where the POA is running.

- "Setting Up the POA Web Console" on page 489
- "Accessing the POA Web Console" on page 491
- "Monitoring the POA from the POA Web Console" on page 492
- "Controlling the POA from the POA Web Console" on page 495

Setting Up the POA Web Console

The default HTTP port for the POA Web console is established during POA installation. You can change the port number and increase security after installation in ConsoleOne.

1. In ConsoleOne, browse to and right-click the POA object, then click Properties.
2. Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 172.16.5.18

Proxy Server Address:

IPX/SPX Address:

	Port	SSL	SSL Port
Message Transfer:	7101	Disabled	
HTTP:	7181	Disabled	
Local Intranet Client/Server:	1677	Disabled	
Internet Proxy Client/Server:	0	Disabled	
IMAP:	144	Disabled	993
CAP:	1026	Disabled	

If you configured the POA for TCP/IP links during installation, the TCP/IP Address field should display the POA server's network address. If it does not, follow the instructions in "Using TCP/IP Links between the Post Office and the Domain" on page 443. The POA must be configured for TCP/IP in order to provide the POA Web console.

3 Make a note of the IP address or DNS hostname in the TCP/IP Address field. You need this information to access the POA Web console.

The HTTP Port field displays the default port number of 7181.

4 If the default HTTP port number is already in use on the POA server, specify a unique port number.

5 Make a note of the HTTP port number. You need this information to access the POA Web console.

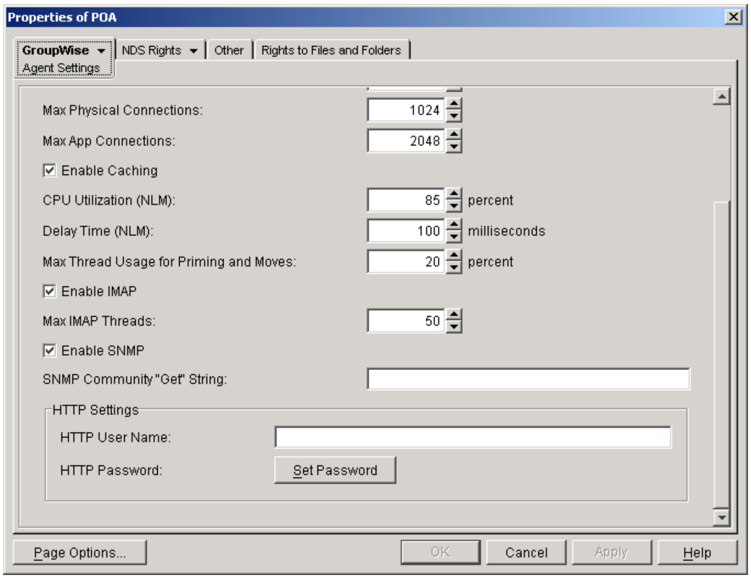
6 If you want to use an SSL connection for the POA Web console, select Enabled in the HTTP SSL drop-down list.

For additional instructions about using SSL connections, see Chapter 80, "Encryption and Certificates," on page 1039.

7 Click Apply to save your changes on the Network Address page.

If you want to limit access to the POA Web console, you can provide a username and password.

8 Click GroupWise > Agent Settings, then scroll down to HTTP Settings.



Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

☑ Enable SNMP

SNMP Community "Get" String:

HTTP User Name:

HTTP Password:

9 In the HTTP Settings box:

9a In the HTTP User Name field, specify a unique username.

9b Click Set Password.

9c Type the password twice for verification.

9d Click Set Password.

Unless you are using an SSL connection, do not use Novell® eDirectory™ username and password because the information passes over the insecure connection between your Web browser and the POA.

For convenience, use the same username and password for all agents that you plan to monitor from GroupWise Monitor. This saves you from having to provide the username and password information as Monitor accesses each agent.

10 Click OK to save the POA Web console settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches

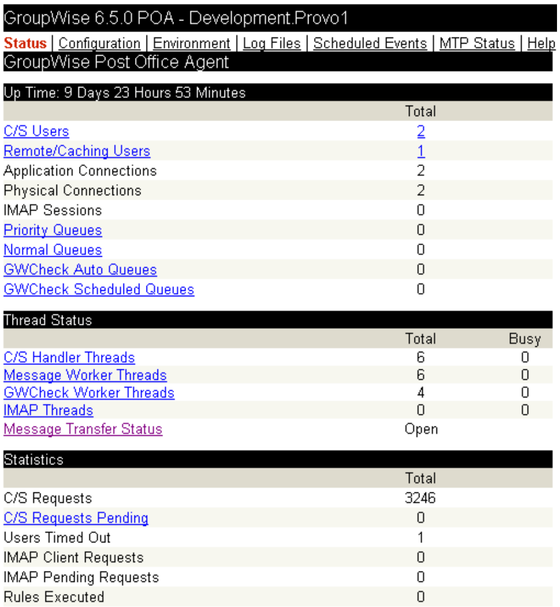
You could also use the /httpport, /httpuser, /httppassword, and /httpssl startup switches in the POA startup file to enable and secure the POA Web console. In addition, you can use the /httprefresh switch to control how often the POA refreshes the information provided to your Web browser.

Accessing the POA Web Console

To monitor the POA from your Web browser, view the POA Web console by supplying the network address and port number as displayed on the Network Address page in ConsoleOne. For example:

http://172.16.5.18:1677
http://172.16.5.18:7181
http://server1:7181
https://server2:1677

When viewing the POA Web console, you can specify either the client/server port or the HTTP port.



GroupWise 6.5.0 POA - Development.Provo1

Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

GroupWise Post Office Agent

Up Time: 9 Days 23 Hours 53 Minutes

	Total
C/S Users	2
Remote/Caching Users	1
Application Connections	2
Physical Connections	2
IMAP Sessions	0
Priority Queues	0
Normal Queues	0
GWCheck Auto Queues	0
GWCheck Scheduled Queues	0

Thread Status

	Total	Busy
C/S Handler Threads	6	0
Message Worker Threads	6	0
GWCheck Worker Threads	4	0
IMAP Threads	0	0
Message Transfer Status	Open	

Statistics

	Total
C/S Requests	3246
C/S Requests Pending	0
Users Timed Out	1
IMAP Client Requests	0
IMAP Pending Requests	0
Rules Executed	0

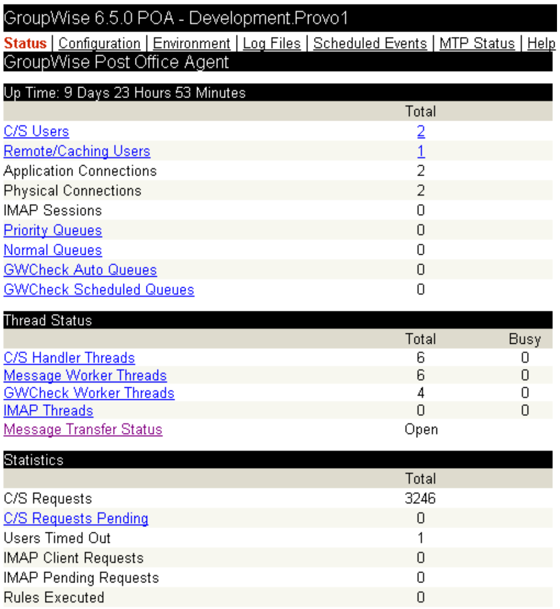
Monitoring the POA from the POA Web Console

The POA Web console provides several pages of information to help you monitor the performance of the POA. The bar at the top of the POA Web console displays the name of the POA and its post office. Below this bar appears the POA Web console menu that lists the pages of information available in the POA Web console. Online help throughout the POA Web console helps you interpret the information being displayed and use the links provided.

- "Monitoring POA Status" on page 492
- "Checking the POA Operating System Environment" on page 493
- "Viewing and Searching POA Log Files" on page 494
- "Listing POA Scheduled Events" on page 494
- "Checking Link Status to the MTA" on page 495

Monitoring POA Status

When you first access the POA Web console, the Status page is displayed. Online help on the Status page helps you interpret the status information being displayed.



GroupWise 6.5.0 POA - Development.Provo1

Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

GroupWise Post Office Agent

Up Time: 9 Days 23 Hours 53 Minutes	Total
C/S Users	2
Remote/Caching Users	1
Application Connections	2
Physical Connections	2
IMAP Sessions	0
Priority Queues	0
Normal Queues	0
GWCheck Auto Queues	0
GWCheck Scheduled Queues	0

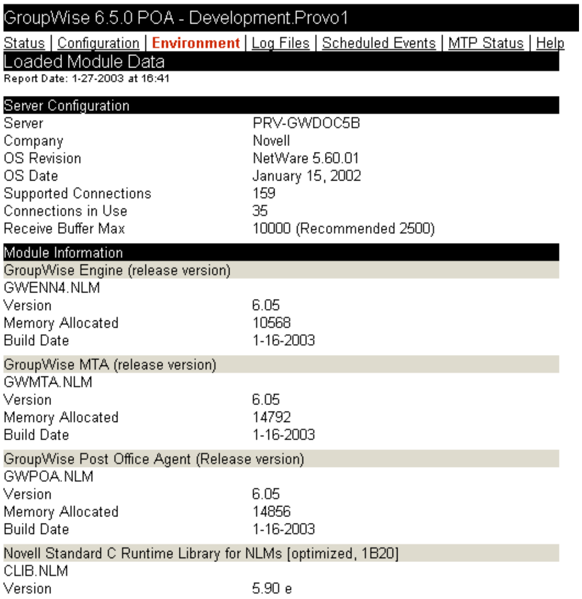
Thread Status	Total	Busy
C/S Handler Threads	6	0
Message Worker Threads	6	0
GWCheck Worker Threads	4	0
IMAP Threads	0	0
Message Transfer Status	Open	

Statistics	Total
C/S Requests	3246
C/S Requests Pending	0
Users Timed Out	1
IMAP Client Requests	0
IMAP Pending Requests	0
Rules Executed	0

Click any hyperlinked status items for additional details. The status information is much the same as that provided at the POA agent console, as described in "Monitoring the POA from the POA Agent Console" on page 475.

Checking the POA Operating System Environment

On the POA Web console menu, click Environment to display information about the operating system where the POA is running. On a NetWare server, the following information is displayed:



GroupWise 6.5.0 POA - Development.Provo1

Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

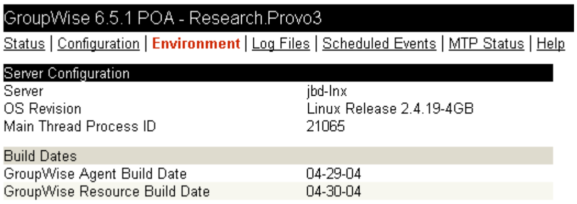
Loaded Module Data

Report Date: 1-27-2003 at 16:41

Server Configuration	
Server	PRV-GWDOC5B
Company	Novell
OS Revision	NetWare 5.60.01
OS Date	January 15, 2002
Supported Connections	159
Connections in Use	35
Receive Buffer Max	10000 (Recommended 2500)

Module Information	
GroupWise Engine (release version)	
GWENN4.NLM	
Version	6.05
Memory Allocated	10568
Build Date	1-16-2003
GroupWise MTA (release version)	
GWMTA.NLM	
Version	6.05
Memory Allocated	14792
Build Date	1-16-2003
GroupWise Post Office Agent (Release version)	
GWPOA.NLM	
Version	6.05
Memory Allocated	14856
Build Date	1-16-2003
Novell Standard C Runtime Library for NLMs [optimized, 1B20]	
CLIB.NLM	
Version	5.90 e

On a Linux server, the following information is displayed:



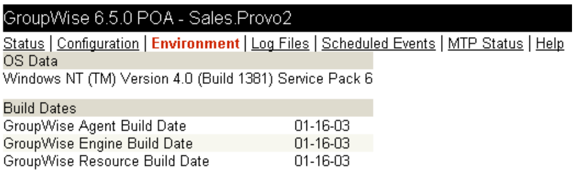
GroupWise 6.5.1 POA - Research.Provo3

Status | Configuration | **Environment** | Log Files | Scheduled Events | MTP Status | Help

Server Configuration	
Server	jbd-lnx
OS Revision	Linux Release 2.4.19-4GB
Main Thread Process ID	21065

Build Dates	
GroupWise Agent Build Date	04-29-04
GroupWise Resource Build Date	04-30-04

On a Windows server, the following information is displayed:



GroupWise 6.5.0 POA - Sales.Provo2

Status | Configuration | **Environment** | Log Files | Scheduled Events | MTP Status | Help

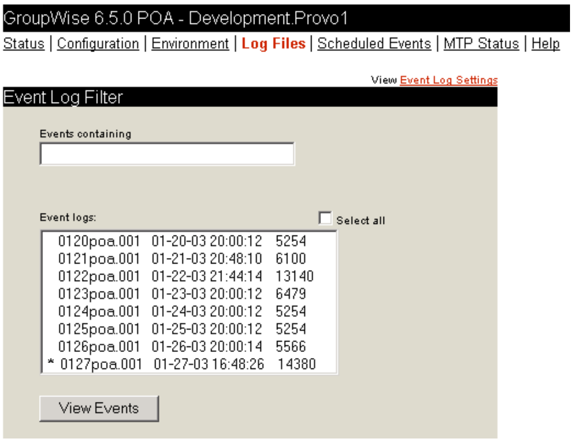
OS Data

Windows NT (TM) Version 4.0 (Build 1381) Service Pack 6

Build Dates	
GroupWise Agent Build Date	01-16-03
GroupWise Engine Build Date	01-16-03
GroupWise Resource Build Date	01-16-03

Viewing and Searching POA Log Files

On the POA Web console menu, click Log Files to display and search POA log files.



GroupWise 6.5.0 POA - Development.Provo1

Status | Configuration | Environment | **Log Files** | Scheduled Events | MTP Status | Help

View Event Log Settings

Event Log Filter

Events containing

Event logs:

□ Select all

```
  0120poa.001  01-20-03 20:00:12  5254
  0121poa.001  01-21-03 20:48:10  6100
  0122poa.001  01-22-03 21:44:14  13140
  0123poa.001  01-23-03 20:00:12  6479
  0124poa.001  01-24-03 20:00:12  5254
  0125poa.001  01-25-03 20:00:12  5254
  0126poa.001  01-26-03 20:00:14  5566
* 0127poa.001  01-27-03 16:48:26  14380
```

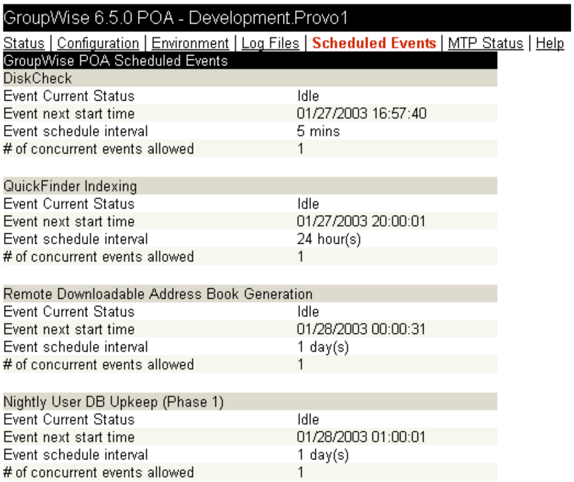
To view a particular log file, select the log file, then click View Events.

To search all log files for a particular string, type the string in the Events Containing field, select Select All, then click View Events. You can also manually select multiple log files to search.

The results of the search are displayed on a separate page which can be printed.

Listing POA Scheduled Events

On the POA Web console menu, click Scheduled Events to view currently scheduled events and their status information.



GroupWise 6.5.0 POA - Development.Provo1

Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

GroupWise POA Scheduled Events

DiskCheck	
Event Current Status	Idle
Event next start time	01/27/2003 16:57:40
Event schedule interval	5 mins
# of concurrent events allowed	1

QuickFinder Indexing	
Event Current Status	Idle
Event next start time	01/27/2003 20:00:01
Event schedule interval	24 hour(s)
# of concurrent events allowed	1

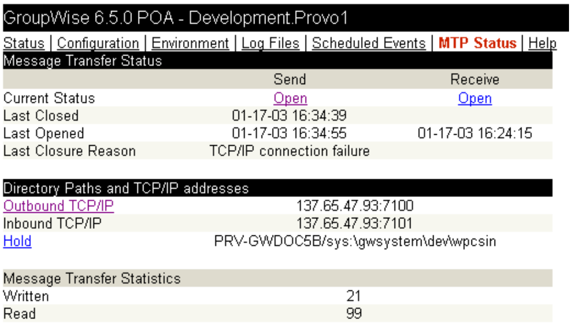
Remote Downloadable Address Book Generation	
Event Current Status	Idle
Event next start time	01/28/2003 00:00:31
Event schedule interval	1 day(s)
# of concurrent events allowed	1

Nightly User DB Upkeep (Phase 1)	
Event Current Status	Idle
Event next start time	01/28/2003 01:00:01
Event schedule interval	1 day(s)
# of concurrent events allowed	1

QuickFinder indexing and remote downloadable Address Book generation can be controlled using links from the Configuration page. The Configuration page also displays information about disk check events and database maintenance events. However, scheduled events must be created and modified using ConsoleOne.

Checking Link Status to the MTA

On the POA Web console menu, click MTP Status to view status information about the link between the POA for the post office and MTA for the domain.



GroupWise 6.5.0 POA - Development.Provo1

Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

Message Transfer Status

	Send	Receive
Current Status	Open	Open
Last Closed	01-17-03 16:34:39	
Last Opened	01-17-03 16:34:55	01-17-03 16:24:15
Last Closure Reason	TCP/IP connection failure	

Directory Paths and TCP/IP addresses	
Outbound TCP/IP	137.65.47.93:7100
Inbound TCP/IP	137.65.47.93:7101
Hold	PRV-GWDOC5B/sys:\gwsystem\dev\wpcsin

Message Transfer Statistics	
Written	21
Read	99

The Outbound TCP/IP link displays the MTA Web console where you can get status information about the MTA. The Hold link displays the contents of the MTA input queue, so you can find out if messages are waiting for processing by the MTA.

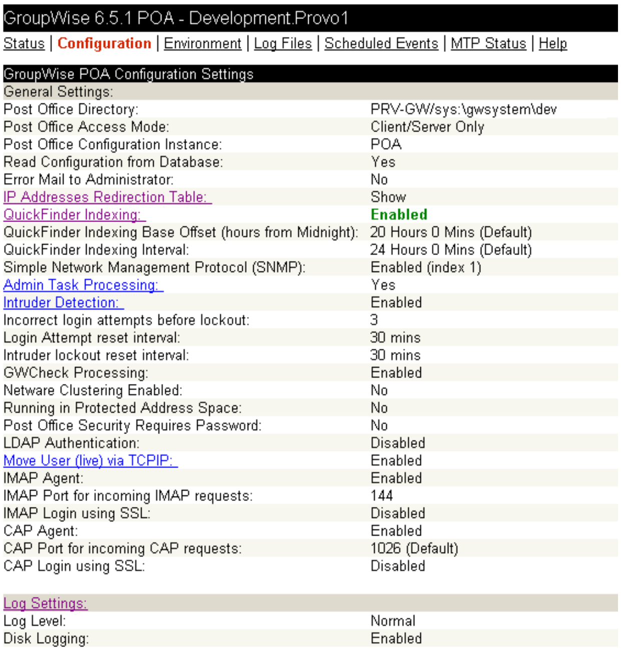
Controlling the POA from the POA Web Console

At the POA Web console, you can change some POA configuration settings for the current POA session. You can also stop and start some specific POA threads.

- "Changing POA Configuration Settings" on page 496
- "Controlling the POA Admin Thread" on page 496
- "Controlling the POA MTP Threads" on page 497

Changing POA Configuration Settings

On the POA Web console menu, click Configuration. Online help on the Configuration page helps you interpret the configuration information being displayed.


GroupWise 6.5.1 POA - Development.Provo1
Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

GroupWise POA Configuration Settings

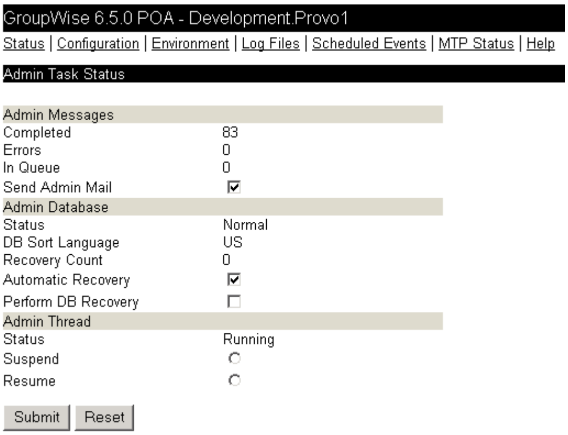
General Settings:	
Post Office Directory:	PRV-GW/sys:\gwsystem\dev
Post Office Access Mode:	Client/Server Only
Post Office Configuration Instance:	POA
Read Configuration from Database:	Yes
Error Mail to Administrator:	No
IP Addresses Redirection Table:	Show
QuickFinder Indexing:	**Enabled**
QuickFinder Indexing Base Offset (hours from Midnight):	20 Hours 0 Mins (Default)
QuickFinder Indexing Interval:	24 Hours 0 Mins (Default)
Simple Network Management Protocol (SNMP):	Enabled (index 1)
Admin Task Processing:	Yes
Intruder Detection:	Enabled
Incorrect login attempts before lockout:	3
Login Attempt reset interval:	30 mins
Intruder lockout reset interval:	30 mins
GWCheck Processing:	Enabled
Netware Clustering Enabled:	No
Running in Protected Address Space:	No
Post Office Security Requires Password:	No
LDAP Authentication:	Disabled
Move User (live) via TCPIP:	Enabled
IMAP Agent:	Enabled
IMAP Port for incoming IMAP requests:	144
IMAP Login using SSL:	Disabled
CAP Agent:	Enabled
CAP Port for incoming CAP requests:	1026 (Default)
CAP Login using SSL:	Disabled

Log Settings:	
Log Level:	Normal
Disk Logging:	Enabled

Click any hyperlinked configuration items to change settings for the current agent session. The settings that can be modified are much the same as those that can be changed at the POA agent console, as described in "Controlling the POA from the POA Agent Console" on page 479.

Controlling the POA Admin Thread

On the Configuration page, click Admin Task Processing.


GroupWise 6.5.0 POA - Development.Provo1
Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

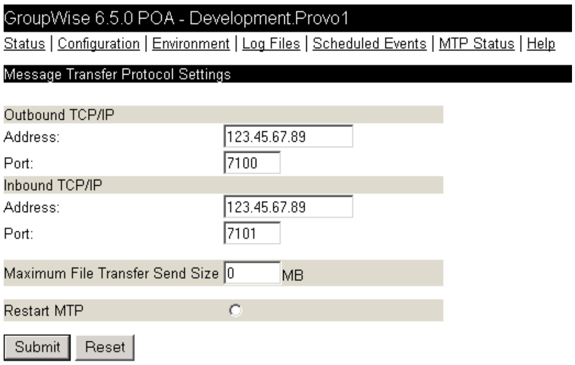
Admin Task Status

Admin Messages	
Completed	83
Errors	0
In Queue	0
Send Admin Mail	☑
Admin Database	
Status	Normal
DB Sort Language	US
Recovery Count	0
Automatic Recovery	☑
Perform DB Recovery	□
Admin Thread	
Status	Running
Suspend	○
Resume	○

Modify the functioning of the POA admin thread as needed, then click Submit. The changes remain in effect for the current POA session.

Controlling the POA MTP Threads

On the Configuration page, click Message Transfer Protocol.


GroupWise 6.5.0 POA - Development.Provo1
Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help
Message Transfer Protocol Settings
Submit
Reset

Outbound TCP/IP
Address: 123.45.67.89
Port: 7100
Inbound TCP/IP
Address: 123.45.67.89
Port: 7101
Maximum File Transfer Send Size 0 MB
Restart MTP ○

On this page, you can restart MTA processing between the POA and the MTA. On the MTP status page, you can restart the send and receive threads separately.

Using POA Log Files

Error messages and other information about POA functioning are written to log files as well as displaying on the POA agent console. Log files can provide a wealth of information for resolving problems with POA functioning or message flow. This section covers the following subjects to help you get the most from POA log files:

- "Configuring POA Log Settings and Switches" on page 497
- "Viewing POA Log Files" on page 498
- "Interpreting POA Log File Information" on page 498

Configuring POA Log Settings and Switches

The following aspects of logging are configurable:

- Log File Path (/log)
- Disk Logging (/logdiskoff)
- Logging Level (/loglevel)
- Maximum Log File Age (/logdays)
- Maximum Log File Size (/logmax)

You can configure the log settings in the following ways:

- Using ConsoleOne to establish defaults (see "Adjusting the POA Logging Level and Other Log Settings" on page 446)
- Using startup switches to override ConsoleOne settings (see "Using POA Startup Switches" on page 523)
- Using the POA agent console to override other settings for the current POA session (see "Adjusting POA Log Settings" on page 488)
- Using the POA Web console to override other settings for the current POA session (see "Controlling the POA from the POA Web Console" on page 495)

Viewing POA Log Files

You can view the contents of the POA log file from the POA agent console and Web console. See the following tasks:

- "Browsing the Current POA Log File" on page 487
- "Viewing a Selected POA Log File" on page 488
- "Cycling the POA Log File" on page 488
- "Viewing and Searching POA Log Files" on page 494

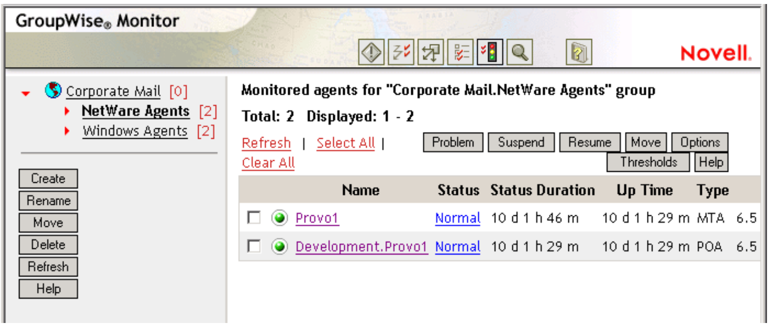
Interpreting POA Log File Information

On startup, the POA records the POA settings currently in effect. Thereafter, it logs events that take place, including errors. To look up error messages that appear in POA log files, see "Post Office Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

Because the POA consists of multiple threads, you might find it useful to retrieve the log file into an editor and sort it on the thread ID that follows the date and time information. Sorting groups all messages together for the same POA thread. You can also use the search capability of the POA Web console to gather information about a specific POA thread. See "Viewing and Searching POA Log Files" on page 494.

Using GroupWise Monitor

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents and gateways from any location where you are connected to the Internet and have access to a Web browser. The POA Web console can be accessed from GroupWise Monitor, enabling you to monitor all POAs in your GroupWise system from one convenient location. In addition, GroupWise Monitor can notify you when agent problems arise.



Monitored agents for "Corporate Mail.NetWare Agents" group

Total: 2 Displayed: 1 - 2

		Name	Status	Status Duration	Up Time	Type	
□	●	Provo1	Normal	10 d 1 h 46 m	10 d 1 h 29 m	MTA	6.5
□	●	Development.Provo1	Normal	10 d 1 h 29 m	10 d 1 h 29 m	POA	6.5

For installation and setup instructions, see "Installing GroupWise Monitor" in the *GroupWise 6.5 Installation Guide*. For usage instructions, see "Monitor" on page 901.

Using NetWare 6.5 Remote Manager

If the POA is running on a NetWare 6.5 server, you can use the IP Address Management feature in NetWare Remote Manager (NetWare Remote Manager > Manage Server > IP Address Management) to view the IP address and port configuration for the POA. This is also true for other GroupWise agents (MTA, Internet Agent, and WebAccess Agent) running on NetWare 6.5 servers.

IMPORTANT: If the POA is running in protected mode, it does not display in NetWare Remote Manager.

You access NetWare Remote Manager by entering the following URL in a Web browser:

```
http://server_address:8008
```

For example:

```
http://137.65.123.11:8008
```

For more information about using NetWare Remote Manager, see the NetWare 6.5 documentation (http://www.novell.com/documentation/nw65).

Using SNMP Monitoring Programs

You can monitor the POA from the Management and Monitoring component of Novell ZENworks® for Servers, ManageWise®, or any other SNMP management and monitoring program. When properly configured, the POA sends SNMP traps to network management consoles for display along with other SNMP monitored programs.

Although the POA is SNMP-enabled by default, the server where the POA is installed must be properly configured to support SNMP, and the POA object in eDirectory must be properly configured as well. To set up SNMP services for your server, complete the following tasks:

- "Setting Up SNMP Services for the POA" on page 499
- "Copying and Compiling the POA MIB File" on page 502
- "Customizing Your ManageWise Installation to Monitor the POA" on page 503
- "Configuring the POA for SNMP Monitoring" on page 503

Setting Up SNMP Services for the POA

Select the instructions for the platform where the POA runs:

- "Setting Up SNMP Services for the NetWare POA" on page 499
- "Setting Up SNMP Services for the Linux POA" on page 500
- "Setting Up SNMP Services for the Windows POA" on page 500

Setting Up SNMP Services for the NetWare POA

The NetWare POA supports SNMP through the SNMP services loaded on the NetWare server. SNMP services are provided through the SNMP NLM. The SNMP NLM initiates and responds to requests for monitoring information and generates trap messages.

If the SNMP NLM is not loaded before the NetWare POA, the POA still loads and functions normally, but SNMP support is disabled. The POA does not attempt to auto-load snmp.nlm.

To load the SNMP NLM manually:

1. Go to the console of each NetWare server where you want to implement SNMP services.

   These servers should already have the GroupWise agents installed.

2. Type the command to load the SNMP NLM:

   Syntax:

   ```
   load snmp v control=x monitor=y trap=z
   ```

where v represents Verbose, meaning to display informational messages, and *x*, *y* and *z* are replaced with your system SNMP community strings for SNMP SETs, GETs and TRAPs).

Example:

```
load snmp v control=private monitor=public trap=all
```

The configuration for the SNMP NLM is found in snmp.cfg and traptarg.cfg in the sys:\etc directory. View the contents of these files for more information.

The TCP/IP NLM automatically loads snmp.nlm, using default values for the community strings. If your system uses different community string values, load snmp.nlm before tcpip.nlm.

3. If the SNMP NLM is already loaded, you can add the control and trap parameters by typing the following at the console prompt:

   ```
   snmp control= trap=
   ```

   To automatically load these commands, include them in the autoexec.ncf file.

   For more information about implementing SNMP services, see your NetWare documentation.

4. Skip to "Copying and Compiling the POA MIB File" on page 502.

Setting Up SNMP Services for the Linux POA

The Linux POA is compatible with NET-SNMP. An older version of SNMP called UCD-SNMP cannot be used with the Linux POA. NET-SNMP comes standard with the versions of Red Hat Linux supported for GroupWise 6.5 for Linux, but it does not come standard with the supported versions of SUSE Linux. If you are using SUSE Linux, you must update to NET-SNMP in order to use SNMP to monitor the Linux POA.

1. Make sure you are logged in as root.
2. If NET-SNMP is not already set up on your Linux server, use the following command to configure SNMP:

   ```
   snmpconf -g basic_setup
   ```

   The snmpconf command creates the snmpd.conf file in one of the following directories, depending on your version of Linux:

   /usr/share/snmp
   /usr/local/share/snmp
   ~/.snmp

3. Locate the snmpd.conf file on your Linux server.
4. In a text editor, open the snmpd.conf file and add the following line:

   dlmod Gwsnmp /opt/novell/gw/agents/lib/libgwsnmp.so

5. Save the snmpd.conf file and exit the text editor.
6. Restart the SNMP daemon (snmpd) to put the changes into effect.
7. Skip to "Copying and Compiling the POA MIB File" on page 502.

Setting Up SNMP Services for the Windows POA

SNMP support is provided for up to eight Windows POAs on the same Windows server. Upon startup, each instance of the POA is dynamically assigned a row in its SNMP table. View the contents of the POA MIB for a description of the SNMP variables in the table. See "Copying and Compiling the POA MIB File" on page 502 for more information about MIB files.

To set up SNMP services for the Windows POA, complete the following tasks:

- "Installing Windows SNMP Support" on page 501
- "Installing GroupWise Agent SNMP Support" on page 501

Installing Windows SNMP Support

For Windows, the SNMP service is usually not included during the initial operating system installation. The SNMP service can be easily added at any time. To add or configure the SNMP service, you must be logged in as a member of the Administrator group.

To add the SNMP service to a Windows NT server:

1. From the Control Panel, double-click Network.
2. Click Services > Add > select SNMP Service.
3. Follow the on-screen prompts. You need your original Windows NT media.

   You are given the opportunity to configure the SNMP service. The only required information for GroupWise is the Trap Destination and Community Name.
4. After the installation is complete, reboot the server.

   For more information about configuring the SNMP service, see your Windows NT documentation.

To add the SNMP service to a Windows 2000 server:

1. From the Control Panel, double-click Add/Remove Programs.
2. Click Add/Remove Windows Components.
3. Select Management and Monitoring Tools.
4. Click Details, then select Simple Network Management Protocol.

Continue with "Installing GroupWise Agent SNMP Support" on page 501.

Installing GroupWise Agent SNMP Support

The GroupWise Agent Installation program includes an option for installing SNMP support. However, if the server where you installed the agents did not yet have SNMP set up, that installation option was not available. Now that you have set up SNMP, you can install GroupWise agent SNMP support.

At the Windows server where you want to install the GroupWise agent SNMP support:

1. Run setup.exe at the root of the *GroupWise 6.5 Administrator* CD. Click Install Products > GroupWise Agents > Install GroupWise Agents.

   or

   Run install.exe from the agents subdirectory on the *GroupWise 6.5 Administrator* CD or in your software distribution directory if you have updated it with the latest GroupWise software.
2. In the Installation Path dialog box, browse to and select the path where the agent software is installed, then select Install and Configure SNMP for GroupWise Agents.
3. To shorten the install time, deselect Install GroupWise Agent Software.

4 Continue through the rest of the installation process as prompted by the Agent Installation program.

The Agent Installation program copies the SNMP support files to the agent installation directory, makes the appropriate Windows registry entries, and restarts the Windows SNMP service.

5 Continue with "Copying and Compiling the POA MIB File" on page 502.

Copying and Compiling the POA MIB File

An SNMP-enabled POA returns information contained in a Management Information Base (MIB). The MIB is an ASCII data structure that defines the information gathered. It also defines the properties that can be monitored and managed on the SNMP-enabled POA.

Before you can monitor an SNMP-enabled POA, you must compile the gwpoa.mib file using your SNMP management program. For NetWare or Windows, the GroupWise MIBs are located on the *GroupWise 6.5 Administrator* CD in the \agents\snmp directory or in the *software_distribution_directory*\agents\snmp directory if you have updated it with the latest GroupWise software. For Linux, the GroupWise MIBs are located on the *GroupWise 6.5 for Linux Administrator* CD in the /agents/snmp directory.

1 Copy the gwpoa.mib file to the location required by your SNMP management program.

For example, ManageWise users would copy the gwpoa.mib file to the \mw\nms\snmpmibs\current directory. ZENworks Server Management users can access the gwpoa.mib file in the software distribution directory.

2 Compile or import the gwpoa.mib file as required by your SNMP management program.

For example, to compile the gwpoa.mib file for ZENworks Server Management:

2a In ConsoleOne, right-click the Site Server object, then click Properties > MIB Pool.

2b Click Modify Pool > Add.

2c Browse to and select the gwpoa.mib file, then click OK.

2d Click Compile.

2e Make sure that the server where the POA is running is configured to send SNMP traps to the ZENworks Server Management Site Server.

- On a NetWare server, add the IP address or hostname of the ZENworks Server Management Site Server to the traptarg.cfg file in the sys:\etc directory.
- On a Windows server, add the IP address or hostname of the ZENworks Server Management Site Server to the list of trap destinations.

  From the Windows NT Control Panel, double-click Network; or, from the Windows 2000 Control Panel, double-click Administrative Tools. Then click Services > SNMP Service > Properties > Traps.

Refer to your SNMP management program documentation for specific instructions.

3 If you are using Novell ManageWise, continue with "Customizing Your ManageWise Installation to Monitor the POA" on page 503.

or

If you are not using ManageWise, skip to "Configuring the POA for SNMP Monitoring" on page 503.

Customizing Your ManageWise Installation to Monitor the POA

The GroupWise agent installation includes files that help ManageWise monitor the GroupWise agents more effectively.

- "GroupWise MIB Files" on page 503
- "GroupWise Agent Alarm Help File" on page 503

These capabilities are available only with ManageWise, not with ZENworks Server Management.

GroupWise MIB Files

The GroupWise MIB files include the standard SNMP management information. In addition, the files include annotations that enhance the Alert functions of ManageWise.

For example, the Summary provides more detailed information than the Description does in other SNMP management programs. The ManageWise annotations are embedded in comments; therefore, they have no affect on other SNMP management programs.

GroupWise Agent Alarm Help File

When GroupWise alarms appear in ManageWise, you can double-click the alarm to display the alarm information contained in the Agent Alarm help file. To enable this feature, copy the gwalarm.hlp file from the \agents\snmp directory to the \mw\nms\help directory on your ManageWise station. This help file explains the alarms each agent might produce by giving a description, cause, and action for each alarm.

Configuring the POA for SNMP Monitoring

In order for SNMP monitoring programs to monitor the POA, the POA must be configured with a network address and SNMP community string.

1. Browse to and right-click the POA object, then click Properties.
2. Click GroupWise > Network Address to display the Network Address page.
3. Click the pencil icon to provide the TCP/IP address or IPX™/SPX™ address of the server where the POA runs, then click Apply.
4. Click GroupWise > Agent Settings page, then scroll to the bottom of the settings list.
5. Provide your system SNMP community GET string, then click OK.

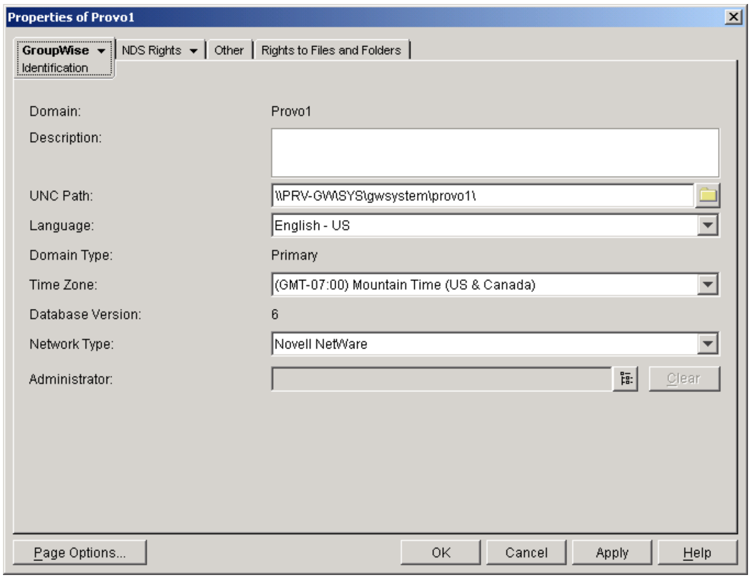
   ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

   The POA should now be visible to your SNMP monitoring program.

Notifying the GroupWise Administrator

If you want to be notified with an e-mail message whenever POAs encounter critical errors, you can designate yourself as an administrator of the domain where the post offices are located.

1. In ConsoleOne, browse to and right-click the Domain object, then click Properties to display the Identification page.



Domain:	Provo1
Description:	
UNC Path:	\\PRV-GW\SYS\gwsystem\provo1\
Language:	English - US
Domain Type:	Primary
Time Zone:	(GMT-07:00) Mountain Time (US & Canada)
Database Version:	6
Network Type:	Novell NetWare
Administrator:	

2 In the Administrator field, browse to and select your GroupWise user ID.

A domain can have a single administrator, or you can create a group of users to function as administrators.

3 Click OK to save the administrator information.

The selected user or group then begins receiving e-mail messages whenever POAs servicing post offices in the domain encounter critical errors.

Corresponding Startup Switches

By default, the POA generates error mail if an administrator has been assigned for the domain. Error mail can be turned off using the /noerrormail switch in the POA startup file.

POA Web Console

Another way to receive e-mail notification of POA problems is to use GroupWise Monitor to access the POA Web console. See "Configuring E-Mail Notification" on page 918.

Using the POA Error Message Documentation

POA error messages are documented with the source and explanation of the error, possible causes of the error, and actions to take to resolve the error. See "Post Office Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

Employing POA Troubleshooting Techniques

If you are having a problem with the POA but not receiving a specific error message, or if the suggested actions for the specific error did not resolve the problem, you can review more general troubleshooting strategies for dealing with POA problems. See "Strategies for Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Using Platform-Specific POA Monitoring Tools

Each operating system where the GroupWise POA runs provides tools for monitoring programs.

- "NetWare Monitoring Tools" on page 505
- "Linux Monitoring Tools" on page 505
- "Windows Monitoring Tools" on page 505

NetWare Monitoring Tools

If you are running the POA on NetWare servers, you can use the NetWare Monitor NLM to monitor the effects of the POA on the NetWare server. NetWare 6.*x* provides monitoring tools that you can use from your Web browser. Processor, resource, and memory utilization can be compared to other non-GroupWise NLM programs to determine if the POA NLM program is monopolizing resources. See your NetWare documentation for additional monitoring suggestions.

Linux Monitoring Tools

If you are running the POA on Linux servers, you can use SNMP tools like snmpget and snmpwalk that allow you to retrieve the data about all the services registered with the SNMP service. These tools are part of the NET-SNMP package. See your Linux documentation for additional monitoring suggestions.

Windows Monitoring Tools

If you are running the POA on Windows servers, you can use the Performance Monitor in Windows Administrator Tools to gather similar information. See your Windows documentation for additional monitoring suggestions.

39 Optimizing the POA

You can adjust how the POA functions to optimize its performance. Before attempting optimization, you should run the POA long enough to observe its efficiency and its impact on other network applications running on the same server. See Chapter 38, "Monitoring the POA," on page 475.

Also, remember that optimizing your network hardware and operating system can make a difference in POA performance.

The following topics help you optimize the POA:

- "Optimizing Client/Server Processing" on page 507
- "Optimizing Message File Processing" on page 511
- "Optimizing Indexing" on page 514
- "Optimizing Database Maintenance" on page 517
- "Optimizing CPU Utilization for the NetWare POA" on page 520

Optimizing Client/Server Processing

If you run only one POA for the post office, you can adjust the number of POA threads and connections for client/server processing. If client/server processing needs are extremely heavy for a post office, you can set up a dedicated client/server POA to meet those needs.

- "Adjusting the Number of POA Threads for Client/Server Processing" on page 507
- "Adjusting the Number of Connections for Client/Server Processing" on page 508
- "Configuring a Dedicated Client/Server POA" on page 510

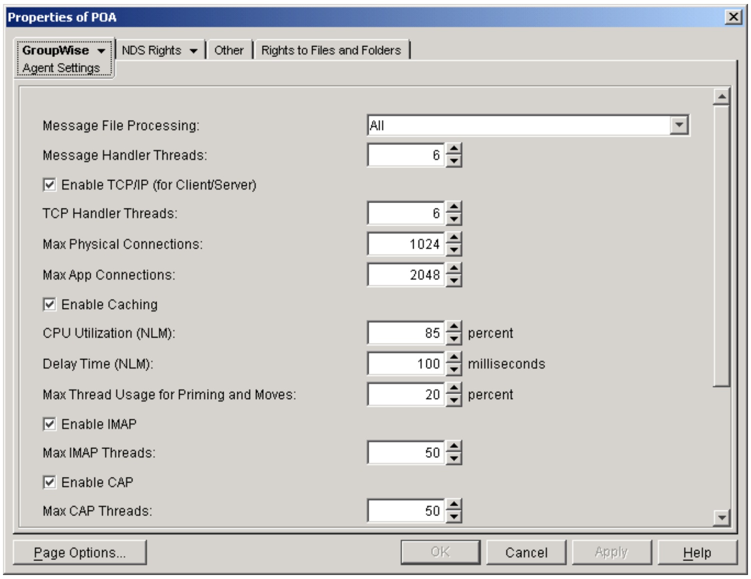
Adjusting the Number of POA Threads for Client/Server Processing

If the POA is configured with client/server processing enabled, it starts TCP handler threads to respond to current client/server requests, up to the number of threads specified by the TCP Handler Threads option. To respond to occasional heavy loads, the POA can increase the number of TCP handler threads above the specified amount if CPU utilization is below the threshold established by the CPU Utilization setting. When the POA rereads its configuration information, the number of TCP handler threads drops back within the configured limit. You can determine how often this happens by checking the Client/Server Pending Requests History page at the POA Web console.

If the POA is frequently not keeping up with the client/server requests from GroupWise® client users, you can increase the maximum number of TCP handler threads so the POA run create additional threads regularly. The default is 6 TCP handler threads; valid values range from 1 to 99.

If GroupWise client users cannot connect to the POA immediately or if response is sluggish, you can increase the number of threads.

1. In ConsoleOne®, browse to and right-click the POA object, then click Properties.
2. Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All

Message Handler Threads: 6

☑ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 6

Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

☑ Enable CAP

Max CAP Threads: 50

3. Increase the number in the TCP Handler Threads field to increase the maximum number of threads the POA can create for client/server processing.

   The optimum number of threads for a POA is affected by many factors, including available system resources, number of users in Caching mode, number of users priming Caching mailboxes, and so on.

   Plan on at least one TCP handler thread per 20-30 client/server users. Or, you can increase the number of TCP handler threads in increments of three to five threads until acceptable throughput is reached. Another approach would be to set the value high initially and then monitor thread usage with the C/S Handler Threads link on the Status page of the POA Web console. If some of the threads always have a count of 0 (zero), meaning they are never used, you can decrease the number of TCP handler threads accordingly.

4. Click OK to save the new thread setting.

   ConsoleOne then notifies the POA to restart so the new thread setting can be put into effect.

Corresponding Startup Switches

You could also use the /tcpthreads switch in the POA startup file to adjust the number of POA threads.

POA Web Console

The Status page helps you assess whether the POA is currently meeting the client/server needs of the post office. Under the Thread Status heading, click C/S Handler Threads to display the workload and status of the client/server handler threads.

You can change the number of client/server handler threads on the Configuration page. Under Performance Settings, click Client/Server Processing Threads.

Adjusting the Number of Connections for Client/Server Processing

Connections are the number of “sockets” through which client/server requests are communicated from the GroupWise client to the POA.

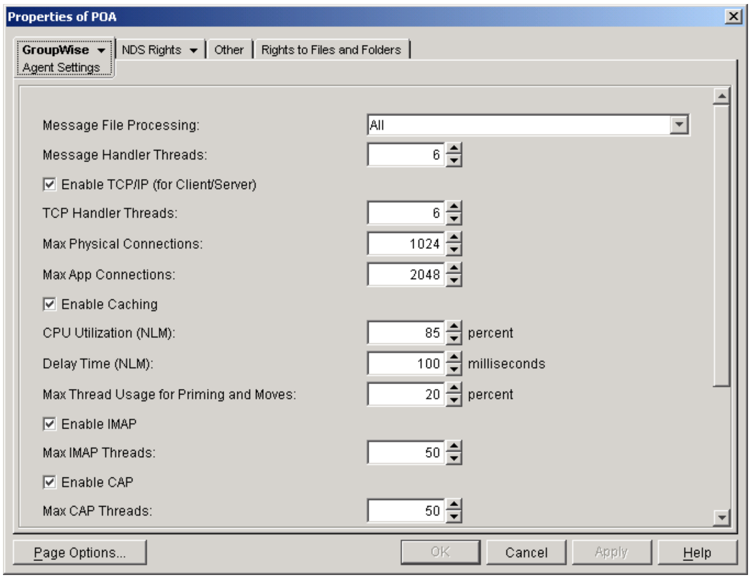
- **Application connections:** Each GroupWise user uses one application connection when he or she starts GroupWise. Depending on what activities the user is doing in the GroupWise client, additional application connections are used. For example, the GroupWise Address Book and GroupWise Notify use individual application connections. The default maximum number of application connections is 2048. You should plan about 3 to 4 application connections per user, so the default is appropriate for a post office of about 500 users.

- **Physical connections:** Each GroupWise user could have zero or multiple active physical connections. One physical connection can accommodate multiple application connections. Inactive physical connections periodically time out and are then closed by the clients and the POA. The default maximum number of physical connections is 1024. You should plan about 1 to 2 physical connections per user, so the default is appropriate for a post office of about 500 users.

If the POA is configured with too few connections to accommodate the number of users in the post office, the POA can encounter an error condition such as "GWPOA: Application connection table full".

1 In ConsoleOne®, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All

Message Handler Threads: 6

☑ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 6

Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

☑ Enable CAP

Max CAP Threads: 50

3 Increase the number in the Max Physical Connections field to increase the amount of TCP/IP traffic the POA can accommodate.

4 Increase the number in the Max App Connections field to increase the number of activities the attached users can perform concurrently.

5 Click OK to save the new connection settings.

ConsoleOne then notifies the POA to restart so the new connection settings can be put into effect.

Corresponding Startup Switches

You could also use the /maxappconns and /maxphysconns switches in the POA startup file to adjust the POA client/server processing.

POA Web Console

The Status page helps you assess whether the POA is currently meeting the client/server needs of the post office. Under the Statistics heading, click C/S Requests Pending. You can also manually select multiple log files to search in order to display a history of times during the last 24 hours when the POA was unable to respond immediately to client/server requests.

Configuring a Dedicated Client/Server POA

When GroupWise users access the post office in client/server mode, the responsiveness of the GroupWise client depends entirely on the ability of the POA to handle the load placed upon it by the users. When you configure a dedicated client/server POA, GroupWise client users do not compete with other POA activities.

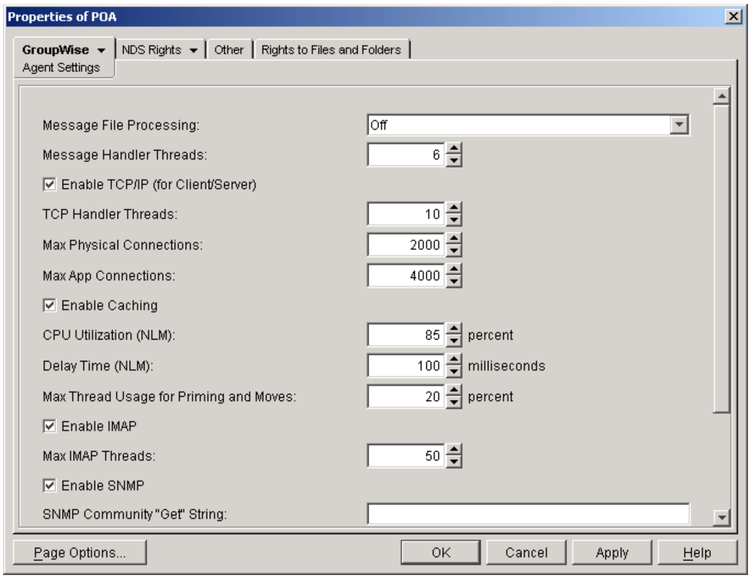
Because many POA functions are disabled when a POA is dedicated to client/server processing, you must run at least one other POA for the post office to take care of the POA functions that the dedicated client/server POA is not performing. This additional POA could be a multipurpose POA, or you could configure additional POAs dedicated to specific types of processing.

To configure a dedicated client/server POA:

1 Create a new POA object for the post office as described in "Creating a POA Object in eDirectory" on page 438.

2 Right-click the new POA object, then click Properties.

3 Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: Off

Message Handler Threads: 6

☑ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 10

Max Physical Connections: 2000

Max App Connections: 4000

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

☑ Enable SNMP

SNMP Community "Get" String:

4 Make sure Enable TCP/IP (for Client/Server) is selected.

5 Increase the number in the TCP Handler Threads field as needed to increase the maximum number of threads the POA can create.

The optimum number of threads for a POA is affected by many factors, including available system resources, number of users in Caching mode, number of users priming Caching mailboxes, and so on.

Plan on at least one TCP handler thread per 20-30 client/server users. Or, you can increase the number of TCP handler threads in increments of three to five threads until acceptable throughput is reached. Another approach would be to set the value high initially and then monitor thread usage with the C/S Handler Threads link on the Status page of the POA Web console. If some of the threads always have a count of 0 (zero), meaning they are never used, you can decrease the number of TCP handler threads accordingly.

6. Increase the number in the Max Physical Connections field as needed to increase the amount of TCP/IP traffic the POA can accommodate.

   Plan on one to two physical connections per user in the post office.

7. Increase the number in the Max App Connections field as needed to increase the number of activities the attached users can perform concurrently.

   Plan on three to four application connections per user in the post office.

8. Set Message File Processing to Off. Make sure another POA handles message file processing.

9. Click Apply to save the updated information on the Agent Settings page.

10. Click GroupWise > QuickFinder.

11. Deselect Enable QuickFinder Indexing, then click Apply. Make sure another POA handles indexing.

12. Click GroupWise > Maintenance.

13. Deselect Enable Automatic Database Recovery. Make sure another POA handles database recovery.

    To turn off all POA admin thread activity, add the /noada switch to the POA startup file for this dedicated client/server POA.

14. Set Maintenance Handler Threads to 0 (zero). Make sure another POA handles database maintenance and disk space management.

15. Deselect Perform User Upkeep and deselect Generate Address Book for Remote. Make sure another POA handles these tasks.

16. Click OK to save the new settings for dedicated client/server processing.

17. Install the POA software on a *different* server from where the original POA for the post office is already running. See "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

18. Add the /name switch to the POA startup file and specify the name designated when you created the new POA object. Also add the /name switch to the startup file for the original POA.

19. Start the dedicated client/server POA. See "Starting the POA" on page 431.

Corresponding Startup Switches
You could also use the /nomf, /noqf, /norecover, /nogwchk, /nonuu, and /nordab switches in the POA startup file to disable non-client/server processing, then use the /tcpthreads, /maxappconns, and /maxphysconns switches to adjust the POA client/server processing.

Optimizing Message File Processing

If you run only one POA for the post office, you can adjust the number of POA threads for message file processing. If message file processing needs are extremely heavy for a post office, you can set up a dedicated message file processing POA to meet those needs.

- "Adjusting the Number of POA Threads for Message File Processing" on page 512

- “Configuring a Dedicated Message File Processing POA” on page 513

Adjusting the Number of POA Threads for Message File Processing

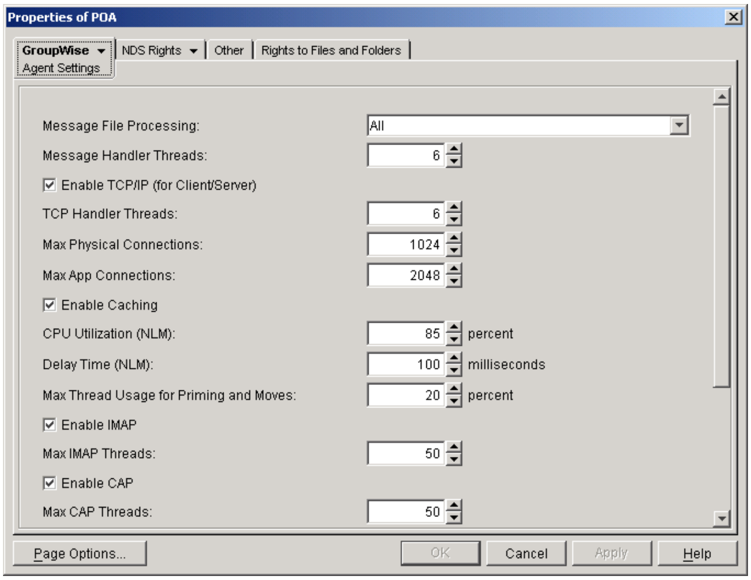
If the POA is configured for message file processing, it starts the number of threads specified by the Message Handler Threads option. Message handler threads deliver messages to users’ mailboxes. The default number of message handler threads is 8; valid values range from 1 to 30.

The more message threads the POA uses, the faster it can process messages. However, the more threads the POA uses, the fewer resources are available to other processes running on the server.

To adjust the number of POA message handler threads:

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All

Message Handler Threads: 6

☑ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 6

Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

☑ Enable CAP

Max CAP Threads: 50

3 Increase the number in the Message Handler Threads field.

For example, you could increase the number of threads in increments of three to five threads until acceptable throughput is reached. The optimum number of threads for a POA is affected by many factors, including available system resources.

4 Click OK to save the new thread setting.

ConsoleOne then notifies the POA to restart so the new setting can be put into effect.

Corresponding Startup Switches

You could also use the /threads switch in the POA startup file to adjust the number of message handler threads.

POA Web Console

The Status page helps you assess whether the POA is currently meeting the message file processing needs of the post office. Under the Thread Status heading, click Message File Processing Threads to display the workload and status of the message handler threads.

You can change the number of message handler threads on the Configuration page. Under Performance Settings, click Message File Processing Threads.

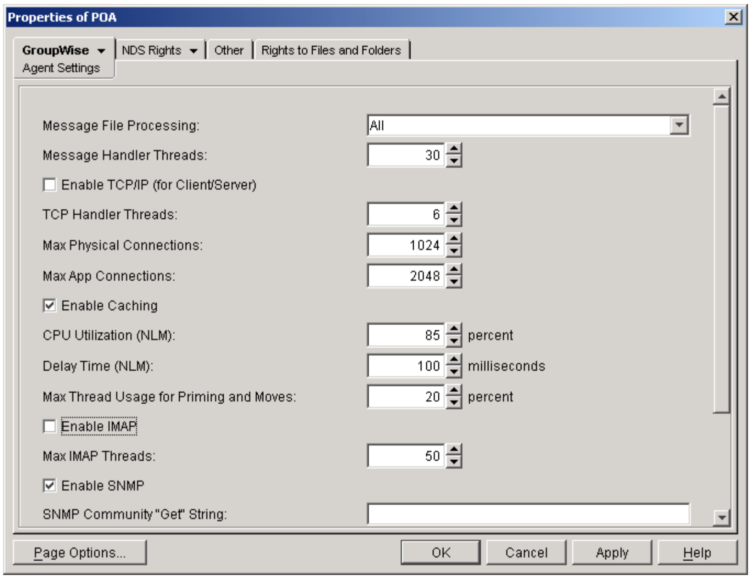
Configuring a Dedicated Message File Processing POA

If client/server processing is being handled by a dedicated client/server POA, you can set up one or more other POAs to handle other POA functions such as message file processing.

1 Create a new POA object for the post office as described in "Creating a POA Object in eDirectory" on page 438.

2 Right-click the new POA object, then click Properties.

3 Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All

Message Handler Threads: 30

□ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 6

Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

□ Enable IMAP

Max IMAP Threads: 50

☑ Enable SNMP

SNMP Community "Get" String:

4 Set Message File Processing to the desired level for this message file processing POA.

If you are using just one message file processing POA, set Message File Processing to All.

For additional load balancing, you could set up two message file processing POAs, one with Message File Processing set to High to handle Busy Searches and requests from Remote client users promptly, and a second with Message File Processing set to Low to handle regular message delivery in the post office.

5 Increase the number in the Message Handler Threads field as needed.

You can configure as many as 30 message handler threads. The optimum number is affected by many factors, including available system resources.

6 Deselect Enable TCP/IP (for Client/Server). Make sure another POA handles client/server processing.

7 Click Apply to save the updated information on the Agent Settings page.

8 Click GroupWise > QuickFinder.

9 Deselect Enable QuickFinder Indexing, then click Apply. Make sure another POA handles indexing.

10 Click GroupWise > Maintenance.

11 Deselect Enable Automatic Database Recovery. Make sure another POA handles database recovery.

To turn off all POA admin thread activity, add the /noada switch to the POA startup file for this dedicated message file processing POA.

12 Set Maintenance Handler Threads to 0 (zero). Make sure another POA handles database maintenance and disk space management.

13 Deselect Perform User Upkeep and deselect Generate Address Book for Remote. Make sure another POA handles these tasks.

14 Click OK to save the new settings for dedicated message file processing.

15 Install the POA software on a *different* server from where the original POA for the post office is already running. See "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

16 Add the /name switch to the POA startup file and specify the name designated when the new POA object was created. Also add the /name switch to the startup file for the original POA.

17 Start the dedicated message file processing POA. See "Starting the POA" on page 431.

Corresponding Startup Switches

You could also use the /notcpip, /noqf, /norecover, /nogwchk, /nonuu, and /nordab switches in the POA startup file to disable non-message file processing, then use the /nomfhigh and /nomflow switches in the POA startup file to adjust the POA message file processing.

Optimizing Indexing

If you run only one POA for the post office, you can adjust the indexing schedule. If indexing needs are extremely heavy for a post office, you can set up a dedicated indexing POA to meet those needs.

- "Regulating Indexing" on page 514
- "Configuring a Dedicated Indexing POA" on page 516

NOTE: To facilitate the Find feature in the GroupWise client, the POA searches unindexed messages as well as those that have already been indexed, so that all messages are immediately available to users whenever they perform a search. The POA does not search unindexed documents, so documents cannot be located using the client Find feature until after indexing has been performed.

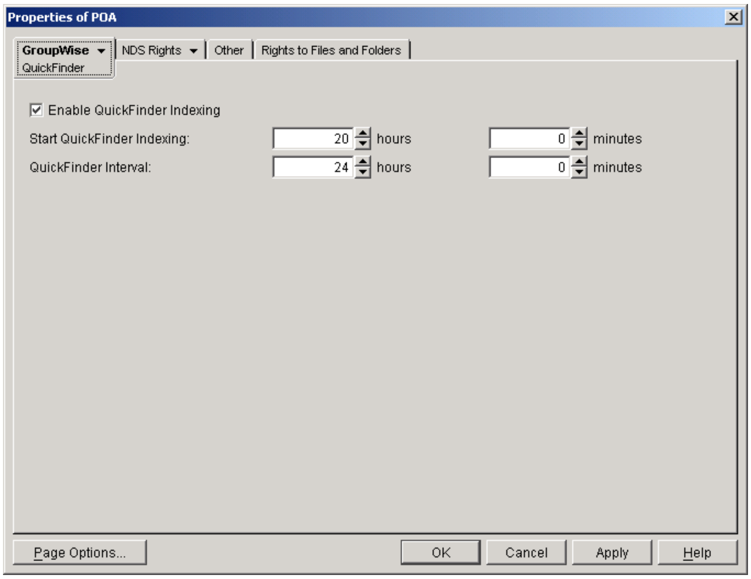
Regulating Indexing

By default, the POA indexes messages and documents in the post office every 24 hours at 8:00 p.m. You can modify this interval if users need messages and documents indexed more quickly. To start indexing immediately, see "Updating QuickFinder Indexes" on page 486.

To adjust the interval at which indexing occurs:

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > QuickFinder to display the QuickFinder page.



☑ Enable QuickFinder Indexing

Start QuickFinder Indexing: 20 hours 0 minutes

QuickFinder Interval: 24 hours 0 minutes

3 Make sure Enable QuickFinder Indexing is selected.

4 In the Start QuickFinder Indexing field, specify the number of hours and minutes after midnight you want the POA to start its indexing cycle.

For example, if you set QuickFinder Interval to 6 and Start QuickFinder Indexing to 1 hour, indexing cycles would occur at 1:00 a.m., 7:00 a.m., 1:00 p.m., and 7:00 p.m.

5 Decrease the number of hours and minutes in the QuickFinder Interval field so indexing occurs more frequently.

The interval is measured from the start of one indexing cycle to the next, so that indexing starts at regular intervals, no matter how long each indexing session takes. By default, the start point of the cycle is 8:00 p.m.

To avoid overloading the POA with indexing processing, a maximum of 500 items are indexed per database for each indexing cycle. If a very large number of messages are received regularly, you should configure the POA with frequent indexing cycles in order to get all messages indexed in a timely manner.

To handle occasional heavy indexing requirements, you can start indexing manually. See "Updating QuickFinder Indexes" on page 486.

6 Click OK to save the new indexing settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches

You could also use the /qfinterval, /qfintervalinminute, /qfbaseoffset, and /qfbaseoffsetinminute switches in the POA startup file to regulate indexing.

POA Web Console

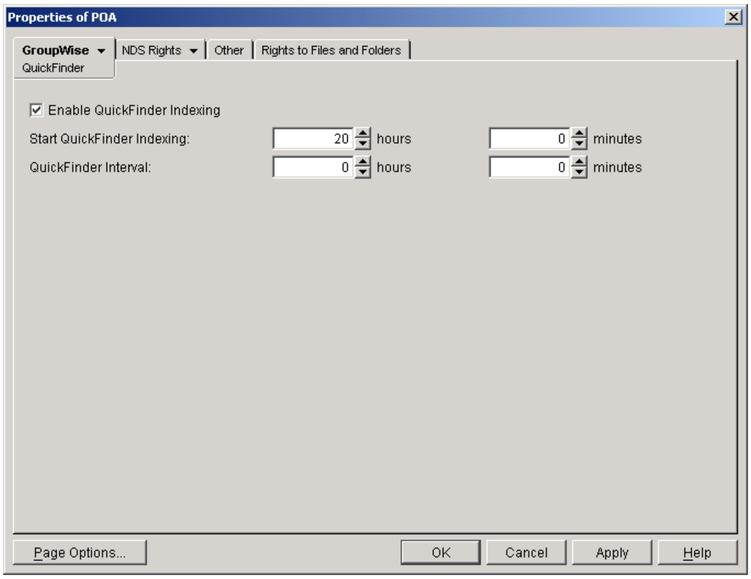
You can control indexing for the current POA session on the Configuration page. Under the General Settings heading, click QuickFinder Indexing. If indexing is currently in progress, you can check the status of the indexing process on the Scheduled Events page.

Configuring a Dedicated Indexing POA

If your GroupWise client users rely heavily on indexed documents, you can set up a dedicated indexing POA so that indexing can be done quickly without impacting other POA functions. The steps provided in this section would be appropriate for a basic indexing POA. For a discussion of more complex configuration options, see "Indexing Documents" on page 319.

To configure a basic dedicated indexing POA:

1. Create a new POA object for the post office as described in "Creating a POA Object in eDirectory" on page 438.
2. Right-click the new POA object, then click Properties.
3. Click GroupWise > QuickFinder to display the QuickFinder page.



☑ Enable QuickFinder Indexing

Start QuickFinder Indexing: 20 hours 0 minutes

QuickFinder Interval: 0 hours 0 minutes

4. Make sure Enable QuickFinder Indexing is selected.
5. In the Start QuickFinder Indexing field, specify the number of hours and minutes after midnight you want the POA to start its indexing cycle.

   The default is 20, meaning at 8:00 p.m.
6. Set QuickFinder Update Interval low enough to keep up with the indexing demands of your GroupWise client users.

   To avoid overloading the POA with indexing processing, a maximum of 500 items are indexed per database for each indexing cycle. If a very large number of messages are received regularly, you should configure the POA with very frequent indexing cycles in order to get all messages indexed in a timely manner.

   For continuous QuickFinder™ indexing, set QuickFinder Update Interval to 0 (zero).
7. Click Apply to save the updated QuickFinder settings.
8. Click GroupWise > Agent Settings.
9. Set Message File Processing to Off. Make sure another POA handles message file processing.
10. Deselect Enable TCP/IP (for Client/Server) and set TCP Handler Threads to 0. Make sure another POA handles client/server processing.

11 Click Apply to save the updated agent settings.

12 Click GroupWise > Maintenance.

13 Deselect Enable Automatic Database Recovery. Make sure another POA handles database recovery.

To turn off all POA admin thread activity, add the /noada switch to the POA startup file for this dedicated indexing POA.

14 Set Maintenance Handler Threads to 0 (zero). Make sure another POA handles database maintenance and disk space management.

15 Deselect Perform User Upkeep and deselect Generate Address Book for Remote. Make sure another POA handles these tasks.

16 Click OK to save the new settings for dedicated indexing.

17 Install the POA software on a *different* server from where the original POA for the post office is already running. See "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

18 Add the /name switch to the POA startup file and specify the name designated when the new POA object was created. Also add the /name switch to the startup file for the original POA.

19 Start the dedicated indexing POA. See "Starting the POA" on page 431.

Corresponding Startup Switches
You could also use the /nomf, /notcpip, /norecover, /nonuu, and /nordab switches in the POA startup file to disable unwanted processing, then use the /qfinterval, /qfintervalinminute, /qfbaseoffset, and /qfbaseoffsetinminute switches to control the indexing schedule.

Optimizing Database Maintenance

If you run only one POA for the post office, you can adjust the number of database maintenance threads. If database maintenance needs are extremely heavy for a post office, you can set up a dedicated database maintenance POA to meet those needs.

- "Adjusting the Number of POA Threads for Database Maintenance" on page 517
- "Configuring a Dedicated Database Maintenance POA" on page 518

Adjusting the Number of POA Threads for Database Maintenance

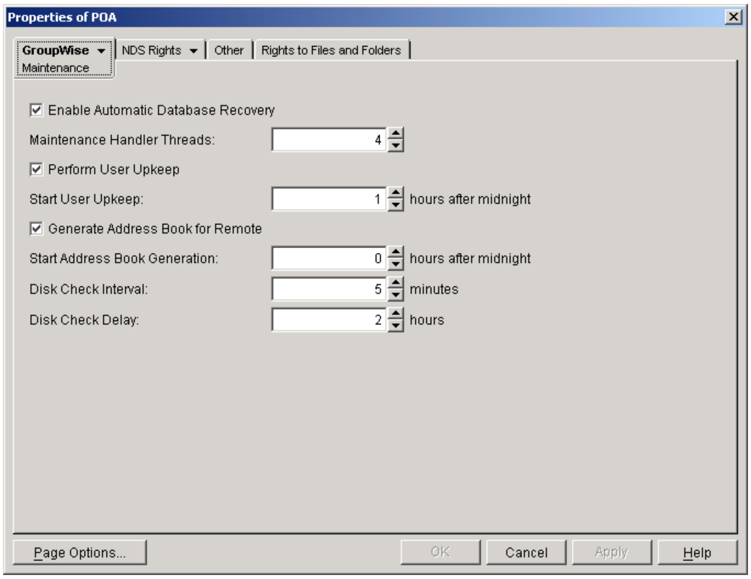
The POA by default performs a certain amount of database maintenance. In addition, you can create your own customized maintenance events as described in "Scheduling Database Maintenance" on page 467 and "Scheduling Disk Space Management" on page 469.

By default, the POA starts one thread to handle all POA scheduled events and also all usage of the Mailbox/Library Maintenance feature in ConsoleOne.

To adjust the number of POA database maintenance handler threads:

1 In ConsoleOne, browse to and right-click the POA object, then click Properties.

2 Click GroupWise > Maintenance to display the Maintenance page.



☑ Enable Automatic Database Recovery

Maintenance Handler Threads: 4

☑ Perform User Upkeep

Start User Upkeep: 1 hours after midnight

☑ Generate Address Book for Remote

Start Address Book Generation: 0 hours after midnight

Disk Check Interval: 5 minutes

Disk Check Delay: 2 hours

3 Increase the number in the Maintenance Handler Threads field.

4 Click OK to save the new thread setting.

ConsoleOne then notifies the POA to restart so the new setting can be put into effect.

Corresponding Startup Switches

You could also use the /gwchkthreads switch in the POA startup file to increase the number of POA threads started for database maintenance activities.

POA Web Console

The Status page helps you assess whether the POA is currently meeting the database maintenance needs of the post office. Under the Thread Status heading, click GWCheck Worker Threads to display the workload and status of the database maintenance handler threads.

You can change the number of database maintenance handler threads on the Configuration page. Under Performance Settings, click Maximum GWCheck Processing Threads.

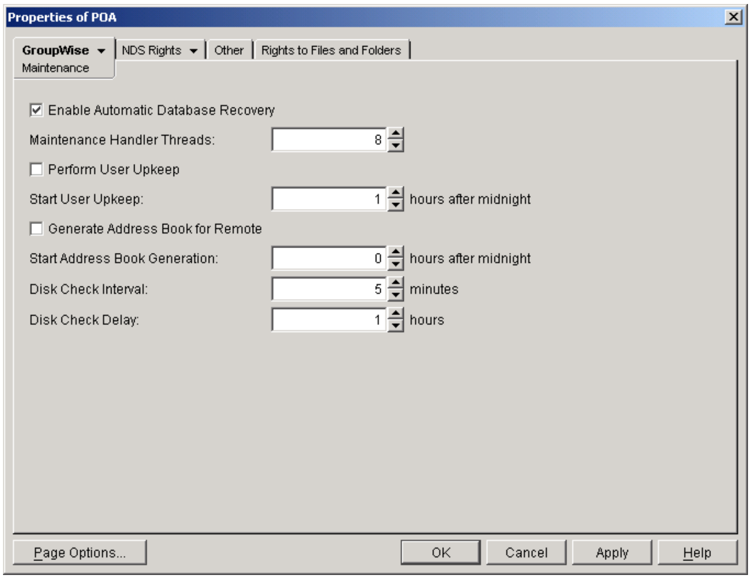
Configuring a Dedicated Database Maintenance POA

If a large amount of database maintenance needs to be performed for a post office, you can set up a dedicated database maintenance POA so that the database maintenance activities do not impact other POA activities, such as responding to GroupWise client users.

1 Create a new POA object for the post office as described in "Creating a POA Object in eDirectory" on page 438.

2 Right-click the new POA object, then click Properties.

3 Click GroupWise > Maintenance to display the Maintenance page.



☑ Enable Automatic Database Recovery

Maintenance Handler Threads: 8

☐ Perform User Upkeep

Start User Upkeep: 1 hours after midnight

☐ Generate Address Book for Remote

Start Address Book Generation: 0 hours after midnight

Disk Check Interval: 5 minutes

Disk Check Delay: 1 hours

4 Make sure Enable Automatic Database Recovery is selected.

5 Set Maintenance Handler Threads as needed.

The maximum number of threads you can start for database maintenance is 8.

6 Deselect Perform User Upkeep and deselect Generate Address Book for Remote. Make sure another POA handles these tasks.

7 Set Disk Check Interval and Disk Check Delay as appropriate for the database maintenance events you plan to schedule.

8 Click Apply to save the updated information on the Maintenance page.

9 Click GroupWise > Scheduled Events, then create database maintenance events as needed, as described in "Scheduling Database Maintenance" on page 467 and "Scheduling Disk Space Management" on page 469.

10 Click GroupWise > Agent Settings.

11 Set Message File Processing to Off. Make sure another POA handles message file processing.

12 Deselect Enable TCP/IP (for Client/Server) and set TCP Handler Threads to 0. Make sure another POA handles client/server processing.

13 Click Apply to save the updated information on the Agent Settings page.

14 Click GroupWise > QuickFinder.

15 Deselect Enable QuickFinder Indexing. Make sure another POA handles indexing.

16 Click OK to save the new settings for dedicated database maintenance processing.

17 Install the POA software on a *different* server from where the original POA for the post office is already running. See "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

18 Add the /name switch to the POA startup file and specify the name designated when you created the new POA object. Also add the /name switch to the startup file for the original POA.

19 Start the dedicated database maintenance POA. See "Starting the POA" on page 431.

Corresponding Startup Switches

You could also use the /nomf, /notcpip, /noqf, /nonuu, and /nordab switches in the POA startup file to disable unwanted processing, then use the /gwchkthreads switch to increase the number of database maintenance handler threads.

Optimizing CPU Utilization for the NetWare POA

To ensure that it does not dominate the NetWare® server CPU, the NetWare POA has a CPU utilization threshold. The default CPU utilization threshold for the NetWare POA is 85 percent. You can change this threshold using the CPU Utilization option. If CPU utilization exceeds the threshold by 5 percent, any idle NetWare POA threads remain idle for the number of milliseconds set by the Delay Time option. This cycle continues until CPU utilization drops below the CPU utilization threshold.

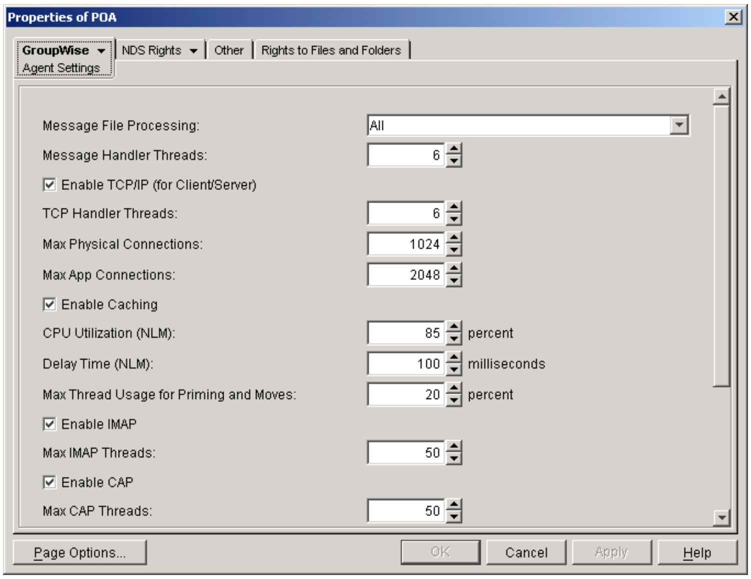
To determine the optimum utilization setting for your network, you must consider the following factors:

- Amount of available memory
- Demands of other network applications
- Type of throughput you want the NetWare POA to provide

As you raise the utilization threshold, NetWare POA efficiency increases; however, other network applications have fewer available resources. As you decrease the utilization threshold, NetWare POA efficiency is reduced; however, the NetWare POA cooperates better with other applications running on the same server. The best way to determine these settings for your network is to experiment.

To adjust the NetWare POA CPU utilization and delay time:

1. In ConsoleOne, browse to and right-click the POA object, then click Properties.
2. Click GroupWise > Agent Settings to display the Agent Settings page.



Message File Processing: All

Message Handler Threads: 6

☑ Enable TCP/IP (for Client/Server)

TCP Handler Threads: 6

Max Physical Connections: 1024

Max App Connections: 2048

☑ Enable Caching

CPU Utilization (NLM): 85 percent

Delay Time (NLM): 100 milliseconds

Max Thread Usage for Priming and Moves: 20 percent

☑ Enable IMAP

Max IMAP Threads: 50

☑ Enable CAP

Max CAP Threads: 50

3. Increase the number in the CPU Utilization field to allow the NetWare POA to use more server resources.

or

Decrease the number in the CPU Utilization field to give the NetWare POA fewer server resources so those resources can be used by other programs on the server.

4 Decrease the number in the Delay Time field to allow NetWare POA threads to take on new tasks more quickly.

or

Increase the number in the Delay Time field to force NetWare POA threads to pause before taking on new tasks.

5 Click OK to save the new CPU utilization settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches

You could also use the /cpu and /sleep switches in the POA startup file to adjust CPU utilization and delay time.

40 Using POA Startup Switches

You can override settings provided in ConsoleOne® by using startup switches. You can override startup switches provided in the startup file by using startup switches on the command line. For more information about starting the POA, see "Starting the POA" on page 431.

The table below summarizes POA startup switches for all platforms and how they correspond to configuration settings in ConsoleOne.

NetWare POA	Linux POA	Windows POA	ConsoleOne Settings
@filename	*@filename*	*@filename*	N/A
/attemptsresetinterval	--attemptsresetinterval	/attemptsresetinterval	Incorrect Login Reset Time
/certfile	--certfile	/certfile	Certificate File
/cap	--cap	/cap	Enable CAP
/capmaxthreads	--capmaxthreads	/capmaxthreads	Max CAP Threads
/capport	--capport	/capport	CAP Port
/capssl	--capssl	/capssl	CAP SSL
/cluster	N/A	N/A	N/A
/cpu	N/A	N/A	CPU Utilization
/dn	N/A	N/A	N/A
/enforceclientversion	--enforceclientversion	/enforceclientversion	Lock Out Older GroupWise Clients
/externalclientssl	--externalclientssl	/externalclientssl	Internet Client/Server SSL
/gwchkthreads	--gwchkthreads	/gwchkthreads	Maintenance Handler Threads
/gwclientreleasedate	--gwclientreleasedate	/gwclientreleasedate	Minimum Client Release Date
/gwclientreleaseversion	--gwclientreleaseversion	/gwclientreleaseversion	Minimum Client Release Version
/help	--help	/help	N/A
/home	--home	/home	N/A
/httppassword	--httppassword	/httppassword	HTTP Password
/httpport	--httpport	/httpport	HTTP Port
/httprefresh	--httprefresh	/httprefresh	N/A

NetWare POA	Linux POA	Windows POA	ConsoleOne Settings
/httpssl	--httpssl	/httpssl	HTTP SSL
/httpuser	--httpuser	/httpuser	HTTP User Name
/imap	--imap	/imap	IMAP
/imapmaxthreads	--imapmaxthreads	/imapmaxthreads	Max IMAP Threads
/imapport	--imapport	/imapport	IMAP Port
/imapreadlimit	--imapreadlimit	/imapreadlimit	N/A
/imapssl	--imapssl	/imapssl	IMAP SSL
/imapsslport	--imapsslport	/imapsslport	IMAP SSL Port
/incorrectloginattempts	--incorrectloginattempts	/incorrectloginattempts	Incorrect Logins Allowed
/internalclientssl	--internalclientssl	/internalclientssl	Local Intranet Client SSL
/intruderlockout	--intruderlockout	/intruderlockout	Enable Intruder Detection
/ip	--ip	/ip	N/A
/keyfile	--keyfile	/keyfile	SSL Key File
/keypassword	--keypassword	/keypassword	SSL Key File Password
/language	--language	/language	N/A
/ldapdisablepwdchg	--ldapdisablepwdchg	/ldapdisablepwdchg	Disable LDAP Password Changing
/ldapipaddr	--ldapipaddr	/ldapipaddr	LDAP Server Address
/ldapippool*n*	--ldapippool*n*	/ldapippool*n*	Select LDAP Servers
/ldappoolresettime	--ldappoolresettime	/ldappoolresettime	LDAP Pool Server Reset Timeout
/ldapport	--ldapport	/ldapport	LDAP Server Address
/ldapportpool*n*	--ldapportpool*n*	/ldapportpool*n*	LDAP Server Address
/ldappwd	--ldappwd	/ldappwd	LDAP Password
/ldapssl	--ldapssl	/ldapssl	Use SSL
/ldapsslpool*n*	--ldapsslpool*n*	/ldapsslpool*n*	Use SSL
/ldapsslkey	--ldapsslkey	/ldapsslkey	SSL Key File
/ldapsslkeypool*n*	--ldapsslkeypool*n*	/ldapsslkeypool*n*	SSL Key File
/ldaptimeout	--ldaptimeout	/ldaptimeout	Inactive Connection Timeout
/ldapuser	--ldapuser	/ldapuser	LDAP User Name
/ldapuserauthmethod	--ldapuserauthmethod	/ldapuserauthmethod	User Authentication Method
/lockoutresetinterval	--lockoutresetinterval	/lockoutresetinterval	Lockout Reset Time

NetWare POA	Linux POA	Windows POA	ConsoleOne Settings
/log	--log	/log	Log File Path
/logdays	--logdays	/logdays	Max Log File Age
/logdiskoff	--logdiskoff	/logdiskoff	Logging Level
/loglevel	--loglevel	/loglevel	Logging Level
/logmax	--logmax	/logmax	Max Log Disk Space
/maxappconns	--maxappconns	/maxappconns	Max Application Connections
/maxphysconns	--maxphysconns	/maxphysconns	Max Physical Connections
/msgtranssl	--msgtranssl	/msgtranssl	Message Transfer SSL
/mtpinipaddr	--mtpinipaddr	/mtpinipaddr	IP Address (POA)
/mtpinport	--mtpinport	/mtpinport	Message Transfer Port (POA)
/mtpoutipaddr	--mtpoutipaddr	/mtpoutipaddr	IP Address (MTA)
/mtpoutport	--mtpoutport	/mtpoutport	Message Transfer Port (MTA)
/mtpsendmax	--mtpsendmax	/mtpsendmax	Maximum Send Message Size
/name	--name	/name	N/A
/noada	--noada	/noada	N/A
/nocache	--nocache	/nocache	Enable Caching
/noconfig	--noconfig	/noconfig	N/A
/noerrormail	--noerrormail	/noerrormail	N/A
/nogwchk	--nogwchk	/nogwchk	N/A
/nomf	--nomf	/nomf	Message File Processing
/nomfhigh	--nomfhigh	/nomfhigh	Message File Processing
/nomflow	--nomflow	/nomflow	Message File Processing
/nomtp	--nomtp	/nomtp	N/A
/nonuu	--nonuu	/nonuu	Perform User Upkeep
/noqf	--noqf	/noqf	Enable QuickFinder Indexing
/nordab	--nordab	/nordab	Generate Address Books for Remote
/norecover	--norecover	/norecover	Enable Auto DB Recovery
/nosnmp	--nosnmp	/nosnmp	Enable SNMP
/notcpip	--notcpip	/notcpip	Enable TCP/IP (for C/S)

NetWare POA	Linux POA	Windows POA	ConsoleOne Settings
/nuuoffset	--nuuoffset	/nuuoffset	Start User Upkeep
/password	--password	/password	Remote Password
/port	--port	/port	Client/Server Port
/primingmax	--primingmax	/primingmax	Max Thread Usage for Priming and Moves
/qfbaseoffset	--qfbaseoffset	/qfbaseoffset	Start QuickFinder Indexing
/qfbaseoffsetinminute	--qfbaseoffsetinminute	/qfbaseoffsetinminute	Start QuickFinder Indexing
/qfinterval	--qfinterval	/qfinterval	QuickFinder Interval
/qfintervalinminute	--qfintervalinminute	/qfintervalinminute	QuickFinder Interval
/rdaboffset	--rdaboffset	/rdaboffset	Start Address Book Generation
/rights	--rights	/rights	N/A
/sleep	N/A	N/A	Delay Time (NLM)
/tcpthreads	--tcpthreads	/tcpthreads	TCP Handler Threads
/threads	--threads	/threads	Message Handler Threads
/user	--user	/user	Remote User Name

@filename

Specifies the location of the POA startup file. On NetWare and Windows, the full path must be included if the file does not reside in the same directory with the POA program. On Linux, the startup file always resides in the /opt/novell/groupwise/agents/share directory. The startup file must reside on the same server where the POA is installed. For more information about the POA startup file, see Chapter 36, “Installing and Starting the POA,” on page 427.

	NetWare POA	Linux POA	Windows POA
Syntax:	@[*vol*:][\dir\\]*file* @\\svr\vol\dir\file	@[/*dir*/]*file*	@[*drive*:][\dir\\]*file* @\\svr\sharename\dir\file
Example:	load gwpoa @sales.poa load gwpoa @sys:\agt\sales.poa load gwpoa @\\s2\sys\agt\sales.poa	./gwpoa @../share/lnxpost.poa	gwpoa.exe @sales.poa gwpoa.exe @d:\agt\sales.poa gwpoa.exe @\\s2\c\agt\sales.poa

/attemptsresetinterval

Specifies the length of time during which unsuccessful login attempts are counted, leading to lockout. The default is 30 minutes; valid values range from 15 to 60. See “Enabling Intruder Detection” on page 465.

	NetWare POA	Linux POA	Windows POA
Syntax:	/attemptsresetinterval-*minutes*	--attemptsresetinterval *minutes*	/attemptsresetinterval-*minutes*
Example:	/attemptsresetinterval-15	--attemptsresetinterval 45	/attemptsresetinterval-60

See also /intruderlockout, /incorrectloginattempts, and /lockoutresetinterval.

/cap

Enables CAP (Calendar Access Protocol) so that the POA can communicate with CAP clients. See "Supporting CAP Clients" on page 451.

	NetWare POA	Linux POA	Windows POA
Syntax:	/cap-enabled or disabled	--cap enabled or disabled	/cap-enabled or disabled
Example:	/cap-enabled	--cap enabled	/cap-enabled

See also /capmaxthreads, /capport, and /capssl.

/capmaxthreads

Specifies the maximum number of CAP threads the POA can create to service CAP clients. The default is 50. This setting is appropriate for most systems. See "Supporting CAP Clients" on page 451.

	NetWare POA	Linux POA	Windows POA
Syntax:	/capmaxthreads-*number*	--capmaxthreads *number*	/capmaxthreads-*number*
Example:	/capmaxthreads-30	--capmaxthreads 40	/capmaxthreads-40

See also /cap, /capport, /capssl.

/capport

Sets the TCP port number used for the POA to communicate with CAP clients. The default is 1026. See "Supporting CAP Clients" on page 451.

	NetWare POA	Linux POA	Windows POA
Syntax:	/capport-*port_number*	--capport *port_number*	/capport-*port_number*
Example:	/capport-1027	--capport 1028	/capport-1028

See also /cap, /capmaxthreads, and /capssl.

/capssl

Sets the availability of secure SSL communication between the POA and CAP clients. Valid settings are enabled and disabled. CAP uses TLS (Transport Layer Security) to negotiate the SSL connection. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/capssl-*setting*	--capssl *setting*	/capssl-*setting*
Example:	/capssl-enabled	--capssl enabled	/capssl-enabled

See also /imap, /imapmaxthreads, and /imapport.

/certfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the POA and other programs. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/certfile-[*svr*\][*vol*:]*dir**file* /certfile-\\*svr**vol**dir**file*	--certfile /*dir*/*file*	/certfile-[*drive*:]*dir**file* /certfile-\\*svr**sharename**dir**file*
Example:	/certfile-\ssl\gw.crt /certfile-server2\sys:\ssl\gw.crt /certfile-\\server2\sys\ssl\gw.crt	--certfile /certs/gw.crt	/certfile-\ssl\gw.crt /certfile-m:\ssl\gw.crt /certfile-\\server2\c\ssl\gw.crt

See also /keyfile and /keypassword.

/cluster

Informs the NetWare® POA that it is running in a Novell cluster. See "Novell Cluster Services" in the *GroupWise 6.5 Interoperability Guide*.

If you are running the NetWare POA on the latest version of NetWare 6.*x* and Novell Cluster Services, the POA can detect the cluster automatically.

	NetWare POA	Linux POA	Windows POA
Syntax:	/cluster	N/A	N/A

See also /ip.

/cpu

Sets the CPU utilization threshold for the NetWare POA. The default is 85 per cent. See "Optimizing CPU Utilization for the NetWare POA" on page 520.

	NetWare POA	Linux POA	Windows POA
Syntax:	/cpu-*percentage*	N/A	N/A
Example:	/cpu-55	N/A	N/A

See also /sleep.

/dn

Specifies the Novell® eDirectory™ distinguished name of the NetWare POA object to facilitate logging into remote servers. It can be used instead of the /user and /password switches.

	NetWare POA	Linux POA	Windows POA
Syntax:	/dn-*distinguished_name*	N/A	N/A
Example:	/dn-POA.sales.provo2	N/A	N/A

/enforceclientversion

Enforces the minimum client release version and/or date so that users of older clients are forced to update in order to access their GroupWise® mailboxes. Valid settings are version, date, both, and disabled. See "Checking What GroupWise Clients Are in Use" on page 452.

	NetWare POA	Linux POA	Windows POA
Syntax:	/enforceclientversion-*setting*	--enforceclientversion *setting*	/enforceclientversion-*setting*
Example:	/enforceclientversion-version	--enforceclientversion date	/enforceclientversion-both

See also /gwclientreleasedate, and /gwclientreleaseversion.

/externalclientssl

Sets the availability of SSL communication between the POA and GroupWise clients that are running outside your firewall. Valid values are enabled, required, and disabled. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/externalclientssl-*setting*	--externalclientssl *setting*	/externalclientssl-*setting*
Example:	/externalclientssl-enabled	--externalclientssl disabled	/externalclientssl-required

See also /certfile, /keyfile, /keypassword, and /port.

/gwchkthreads

Specifies the number of threads the POA starts for Mailbox/Library Maintenance activities. The default is 4; valid values range from 1 to 8. See "Adjusting the Number of POA Threads for Database Maintenance" on page 517.

	NetWare POA	Linux POA	Windows POA
Syntax:	/gwchkthreads-*number*	--gwchkthreads *number*	/gwchkthreads-*number*
Example:	/gwchkthreads-5	--gwchkthreads 6	/gwchkthreads-8

See also /nogwchk.

/gwclientreleasedate

Specifies the date of the approved GroupWise client software for your system. See "Checking What GroupWise Clients Are in Use" on page 452.

	NetWare POA	Linux POA	Windows POA
Syntax:	/gwclientreleasedate-*mm-dd-yyyy*	--gwclientreleasedate *mm-dd-yyyy*	/gwclientreleasedate-*mm-dd-yyyy*
Example:	/gwclientreleasedate-04-02-2001	--gwclientreleasedate 04-28-2004	/gwclientreleasedate-04-02-2001

See also /gwclientreleaseversion and /enforceclientversion.

/gwclientreleaseversion

Specifies the version of the approved GroupWise client software for your system. See "Checking What GroupWise Clients Are in Use" on page 452.

	NetWare POA	Linux POA	Windows POA
Syntax:	/gwclientreleaseversion-*n.n.n*	--gwclientreleaseversion *n.n.n*	/gwclientreleaseversion-*n.n.n*
Example:	/gwclientreleaseversion-6.0.0	--gwclientreleaseversion 6.5.1	/gwclientreleaseversion-6.0.0

See also /gwclientreleasedate and /enforceclientversion.

/help

Displays the POA startup switch Help information. When this switch is used, the POA does not start.

	NetWare POA	Linux POA	Windows POA
Syntax:	/help or /?	--help	/help or /?
Example:	load gwpoa /help	./gwpoa --help	gwpoa.exe /help

/home

Specifies the post office directory, where the POA can find the message and user databases to service. There is no default location. You must use this switch in order to start the POA. See "Starting the POA" on page 431.

	NetWare POA	Linux POA	Windows POA
Syntax:	/home-[*svr*\][*vol*:]*dir* /home-\\*svr**vol**dir*	--home /*dir*	/home-[*drive*:]*dir* /home-\\*svr**sharename**dir*
Example:	/home-\sales /home-mail:\sales /home-server2\mail:\sales /home-\\server2\mail\sales	--home /gwsystem/sales	/home-\sales /home-m:\sales /home-\\server2\c\sales

/httppassword

Specifies the password for the POA to prompt for before allowing POA status information to be displayed in your Web browser. Do not use an existing eDirectory password because the information passes over the insecure connection between your Web browser and the POA. See "Using the POA Web Console" on page 489.

	NetWare POA	Linux POA	Windows POA
Syntax:	/httppassword-*unique_password*	--httppassword *unique_password*	/httppassword-*unique_password*
Example:	/httppassword-AgentWatch	--httppassword AgentWatch	/httppassword-AgentWatch

See also /httpuser, /httpport, /httprefresh, and /httpssl.

/httpport

Sets the HTTP port number used for the POA to communicate with your Web browser. The default is 7181; the setting must be unique. See "Using the POA Web Console" on page 489.

	NetWare POA	Linux POA	Windows POA
Syntax:	/httpport-*port_number*	--httpport *port_number*	/httpport-*port_number*
Example:	/httpport-7182	--httpport 7183	/httpport-7184

See also /httpuser, /httppassword, /httprefresh, and /httpssl.

/httprefresh

Specifies the rate at which the POA refreshes the status information in your Web browser. The default is 60 seconds. See "Using the POA Web Console" on page 489.

	NetWare POA	Linux POA	Windows POA
Syntax:	/httprefresh-*seconds*	--httprefresh *seconds*	/httprefresh-*seconds*
Example:	/httprefresh-30	--httprefresh 90	/httprefresh-120

See also /httpuser, /httppassword, /httpport, and /httpssl.

/httpssl

Sets the availability of secure SSL communication between the POA and the POA Web console displayed in your Web browser. Valid values are enabled and disabled. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/httpssl-*setting*	--httpssl *setting*	/httpssl-*setting*
Example:	/httpssl-enabled	--httpssl enabled	/httpssl-enabled

See also /certfile, /keyfile, and /keypassword.

/httpuser

Specifies the username for the POA to prompt for before allowing POA status information to be displayed in a Web browser. Providing a username is optional. Do not use an existing eDirectory username because the information passes over the insecure connection between your Web browser and the POA. See "Using the POA Web Console" on page 489.

	NetWare POA	Linux POA	Windows POA
Syntax:	/httpuser-*unique_name*	--httprefresh *unique_name*	/httprefresh-*unique_name*
Example:	/httpuser-GWWebCon	--httpuser GWWebCon	/httpuser-GWWebCon

See also /httppassword, /httpport, /httprefresh, and /httpssl.

/imap

Enables IMAP so that the POA can communicate with IMAP clients. Valid settings are enabled and disabled. See "Supporting IMAP Clients" on page 450.

	NetWare POA	Linux POA	Windows POA
Syntax:	/imap-enabled or disabled	--imap enabled or disabled	/imap-enabled or disabled
Example:	/imap-enabled	--imap disabled	/imap-enabled

See also /imapmaxthreads, /imapport, /imapssl, /imapsslport, and /imapreadlimit.

/imapmaxthreads

Specifies the maximum number of IMAP threads the POA can create to service IMAP clients. The default is 50.This setting is appropriate for most systems. See "Supporting IMAP Clients" on page 450.

	NetWare POA	Linux POA	Windows POA
Syntax:	/imapmaxthreads-*number*	--imapmaxthreads *number*	/imapmaxthreads-*number*
Example:	/imapmaxthreads-40	--imapmaxthreads 30	/imapmaxthreads-40

See also /imap, /imapport, /imapssl, /imapsslport, and /imapreadlimit.

/imapreadlimit

Specifies in thousands the maximum number of messages that can be downloaded by an IMAP client. For example, specifying 10 represents 10,000. The default is 5,000

	NetWare POA	Linux POA	Windows POA
Syntax:	/imapreadlimit-*number*	--imapreadlimit *number*	/imapreadlimit-*number*
Example:	/imapreadlimit-10	--imapreadlimit 20	/imapreadlimit-50

See also /imap, /imapmaxthreads, /imapport, /imapssl, and /imapsslport.

/imapport

Sets the TCP port number used for the POA to communicate with IMAP clients when using a non-SSL connection. The default is 143. See "Supporting IMAP Clients" on page 450.

	NetWare POA	Linux POA	Windows POA
Syntax:	/imapport-*port_number*	--imapport *port_number*	/imapport-*port_number*
Example:	/imapport-145	--imapport 146	/imapport-147

See also /imap, /imapmaxthreads, /imapssl, /imapsslport, and /imapreadlimit.

/imapssl

Sets the availability of secure SSL communication between the POA and IMAP clients. Valid settings are enable and disable. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/imapssl-*setting*	--imapssl *setting*	/imapssl-*setting*

	NetWare POA	Linux POA	Windows POA
Example:	/imapssl-enable	--imapssl enable	/imapssl-enable

See also /imap, /imapmaxthreads, /imapport, /imapsslport, and /imapreadlimit.

/imapsslport

Sets the TCP port number used for the POA to communicate with IMAP clients when using an SSL connection. The default is 993. See "Supporting IMAP Clients" on page 450.

	NetWare POA	Linux POA	Windows POA
Syntax:	/imapsslport-*port_number*	--imapsslport *port_number*	/imapsslport-*port_number*
Example:	/imapsslport-994	--imapsslport 995	/imapsslport-996

See also/imap, /imapmaxthreads, /imapport, /imapssl, and /imapreadlimit.

/incorrectloginattempts

Specifies the number of unsuccessful login attempts after which lockout occurs. The default is 5 attempts; valid values range from 3 to 10. See "Enabling Intruder Detection" on page 465.

	NetWare POA	Linux POA	Windows POA
Syntax:	/incorrectloginattempts-*number*	--incorrectloginattempts *number*	/incorrectloginattempts-*number*
Example:	/incorrectloginattempts-3	--incorrectloginattempts 10	/incorrectloginattempts-10

See also /intruderlockout, /attemptsresetinterval, and /lockoutresetinterval.

/internalclientssl

Sets the availability of secure SSL communication between the POA and GroupWise clients that are running inside your firewall. Valid values are enabled, required, and disabled. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/internalclientssl-*setting*	--internalclientssl *setting*	/internalclientssl-*setting*
Example:	/internalclientssl-enabled	--internalclientssl required	/internalclientssl-required

See also /certfile, /keyfile, /keypassword, and /port.

/intruderlockout

Turns on intruder lockout processing, using defaults that can be overridden by the /incorrectloginattempts, /attemptsresetinterval, and /lockoutresetinterval switches. See "Enabling Intruder Detection" on page 465.

	NetWare POA	Linux POA	Windows POA
Syntax:	/intruderlockout	--intruderlockout	/intruderlockout

/ip

Binds the POA to a specific IP address when the server where it runs uses multiple IP addresses, such as in a clustering environment. The specified IP address is associated with all ports used by the POA (HTTP, IMAP, LDAP, and so on.) Without the /ip switch, the POA binds to all available IP addresses and users can access the post office through all available IP addresses. See "Editing Clustered Agent Startup Files" in "Novell Cluster Services" in *GroupWise 6.5 Interoperability Guide*.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ip-*IP_address*	--ip *IP_address*	/ip-*IP_address*
Example:	/ip-172.16.5.18	--ip 172.16.5.18	/ip-172.16.5.18

See also /cluster.

/keyfile

Specifies the full path to the private file used to provide secure SSL communication between the POA and other programs. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/keyfile-[*svr*\][*vol*:]*\dir\file* /keyfile-\\svr\vol\dir\file	--keyfile /*dir*/*file*	/keyfile-[*drive*:]*\dir\file* /keyfile-\\svr\sharename\dir\file
Example:	/keyfile-\ssl\gw.key /keyfile-server2\sys:\ssl\gw.key /keyfile-\\server2\sys\ssl\gw.key	--keyfile /certs/gw.key	/keyfile-\ssl\gw.key /keyfile-m:\ssl\gw.key /keyfile-\\server2\c\ssl\gw.key

See also /certfile and /keypassword.

/keypassword

Specifies the password used to encrypt the private SSL key file when it was created. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/keypassword-*password*	--keypassword *password*	/keypassword-*password*
Example:	/keypassword-gwssl	--keypassword gwssl	/keypassword-gwssl

See also /certfile and /keyfile.

/language

Specifies the language to run the POA in, using a two-letter language code as listed below. You must install the POA in the selected language in order for the POA to display in the selected language.

The initial default is the language used in the post office. If that language has not been installed, the second default is the language used by the operating system. If that language has not been installed, the third default is English. You only need to use this switch if you need to override these defaults.

	NetWare POA	Linux POA	Windows POA
Syntax:	/language-*code*	--language *code*	/language-*code*
Example:	/language-de	--language de	/language-fr

The table below lists the valid language codes. Contact your local Novell sales office for information about language availability.

Language	Language Code	Language	Language Code
Arabic	AR	Hungarian	MA
Czechoslovakian	CS	Italian	IT
Chinese-Simplified	CS	Japanese	NI
Chinese-Traditional	CT	Korean	KR
Danish	DK	Norwegian	NO
Dutch	NL	Polish	PL
English-United States	US	Portuguese-Brazil	BR
Finnish	SU	Russian	RU
French-France	FR	Spanish	ES
German-Germany	DE	Swedish	SV
Hebrew	HE	Turkish	TR

/ldapdisablepwdchg

Prevents GroupWise users from changing their LDAP passwords by using the Password dialog box in the GroupWise client. See "Enabling LDAP Authentication for a Post Office" on page 462.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapdisablepwdchg	--ldapdisablepwdchg	/ldapdisablepwdchg

See also /ldapipaddr, /ldapport, /ldapuser, /ldappwd, /ldapuserauthmethod, /ldapssl, /ldapsslkey, and /ldaptimeout.

/ldapipaddr

Specifies the LDAP server's network address as either an IP address or a DNS hostname. You can specify multiple network addresses to provide failover capabilities for your LDAP servers. See "Specifying Failover LDAP Servers (Non-SSL Only)" on page 465.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapipaddr-*network_address*	--ldapipaddr *network_address*	/ldapipaddr-*network_address*
Example:	/ldapipaddr-172.16.5.18 /ldapipaddr-server1 server2	--ldapipaddr 172.16.5.19 --ldapipaddr server1 server2	/ldapipaddr-172.16.5.20 /ldapipaddr-server1 server2

If you specify multiple LDAP servers, use a space between each address. When so configured, the POA tries to contact the first LDAP server in order to authenticate a user to GroupWise. If that LDAP server is down, the POA tries the next LDAP server in the list, and so on until it is able to authenticate.

See also /ldapport, /ldapuser, /ldappwd, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapssl, /ldapsslkey, and /ldaptimeout.

/ldapippool*n*

Specifies a pooled LDAP server's network address as either an IP address or a DNS hostname. As many as five LDAP servers can participate together as a pool; therefore, *n* ranges from 1 to 5. See "Configuring a Pool of LDAP Servers" on page 464.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapippool*n*-*network_address*	--ldapippool*n* *network_address*	/ldapippool*n*-*network_address*
Example:	/ldapippool1-172.16.5.18 /ldapippool2-server1 /ldapippool3-172.16.5.19	--ldapippool1 172.16.5.18 --ldapippool2 server1 --ldapippool3 172.16.5.19	/ldapippool1-172.16.5.18 /ldapippool2-server1 /ldapippool3-172.16.5.19

See also /ldapportpool*n*, /ldapsslpool*n*, /ldapsslkeypool*n*, and /ldappoolresettime.

/ldappoolresettime

Specifies the number of minutes between the time when the POA receives an error response from a pooled LDAP server and the time when that LDAP server is reinstated into the pool of available LDAP servers. The default is 5 minutes; valid values range from 1 to 30. See "Configuring a Pool of LDAP Servers" on page 464.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldappoolresettime-*minutes*	--ldappoolresettime *minutes*	/ldappoolresettime-*minutes*
Example:	/ldappoolresettime-10	--ldappoolresettime 20	/ldappoolresettime-30

See also /ldapippool*n*, /ldapportpool*n*, /ldapsslpool*n*, and /ldapsslkeypool*n*.

/ldapport

Specifies the port number that the LDAP server listens on for authentication. The default is 389. See "Providing LDAP Authentication for GroupWise Users" on page 461.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapport-*port_number*	--ldapport *port_number*	/ldapport-*port_number*
Example:	/ldapport-390	--ldapport 391	/ldapport-392

See also /ldapipaddr, /ldapuser, /ldappwd, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapssl, /ldapsslkey, and /ldaptimeout.

/ldapportpool*n*

Specifies the port number that pooled LDAP server *n* listens on for authentication. The default is 389. See "Configuring a Pool of LDAP Servers" on page 464.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapportpool*n-port*	--ldapportpool*n port*	/ldapportpool*n-port*
Example:	/ldapportpool2-390	--ldapportpool3 391	/ldapportpool4-392

See also /ldapippool*n*, /ldappoolresettime, /ldapsslpool*n*, and /ldapsslkeypool*n*.

/ldappwd

Provides the password for the LDAP user that the POA uses to log in to the LDAP server. See "Providing LDAP Authentication for GroupWise Users" on page 461.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldappwd-*LDAP_password*	--ldappwd *LDAP_password*	/ldappwd-*LDAP_password*

	NetWare POA	Linux POA	Windows POA
Example:	/ldappwd-gwldap	--ldappwd gwldap	/ldappwd-gwldap

See also /ldapipaddr, /ldapport, /ldapuser, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapssl, /ldapsslkey, and /ldaptimeout.

/ldapssl

Indicates to the POA that the LDAP server it is logging in to is using SSL. See "Providing LDAP Authentication for GroupWise Users" on page 461.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapssl	--ldapssl	/ldapssl

See also /ldapipaddr, /ldapport, /ldapuser, /ldappwd, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapsslkey and /ldaptimeout.

/ldapsslpool*n*

Indicates to the POA that the pooled LDAP server it is logging in to is using SSL. See "Configuring a Pool of LDAP Servers" on page 464.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapsslpool*n*	--ldapsslpool*n*	/ldapsslpool*n*
Example:	/ldapsslpool2	--ldapsslpool3	/ldapsslpool4

See also /ldapippool*n*, /ldapportpool*n*, /ldappoolresettime, and /ldapsslkeypool*n*.

/ldapsslkey

Specifies the full path to the SSL key file used with LDAP authentication. See "Providing LDAP Authentication for GroupWise Users" on page 461.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapsslkey-[*svr*\][*vol*:]\dir\file /ldapsslkey-\\svr\vol\dir\file	--ldapsslkey /*dir*/*file*	/ldapsslkey-[*drive*:]\dir\file /ldapsslkey-\\svr\sharename\dir\file
Example:	/ldapsslkey-\ldap\gwkey.der /ldapsslkey-server2\sys:\ldap\gwkey.der /ldapsslkey-\\\\server2\sys\ldap\gwkey.der	--ldapsslkey /certs/gwkey.der	/ldapsslkey-\ldap\gwkey.der /ldapsslkey-m:\ldap\gwkey.der /ldapsslkey-\\\\server2\c\ldap\gwkey.der

See also /ldapipaddr, /ldapport, /ldapuser, /ldappwd, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapssl and /ldaptimeout.

/ldapsslkeypool*n*

Specifies the full path to the SSL key file used with pooled LDAP server *n* for authentication. See "Configuring a Pool of LDAP Servers" on page 464.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapsslkeypool*n*-[*svr*\][*vol*:]*dir**file* /ldapsslkeypool*n*-\\*svr**vol**dir**file*	--ldapsslkeypool*n*-/*dir*/*file*	/ldapsslkeypool*n*-[*drive*:]*dir**file* /ldapsslkeypool*n*-\\*svr**sharename**dir**file*
Example:	/ldapsslkeypool4-\ldap\gwkey.der /ldapsslkeypool4-svr2\sys:\ldap\gwkey.der /ldapsslkeypool4-\\svr2\sys\ldap\gwkey.der	--ldapsslkeypool4 /certs/gwkey.der	/ldapsslkeypool4-\ldap\gwkey.der /ldapsslkeypool4-m:\ldap\gwkey.der /ldapsslkeypool4-\\svr2\c\ldap\gwkey.der

See also /ldapippool*n*, /ldapportpool*n*, /ldappoolresettime, and /ldapsslpool*n*.

/ldaptimeout

Specifies the number of seconds that the POA connection to the LDAP server can be idle before the POA drops the connection. The default is 30 seconds. See "Providing LDAP Authentication for GroupWise Users" on page 461.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldaptimeout-*seconds*	--ldaptimeout *seconds*	/ldaptimeout-*seconds*
Example:	/ldaptimeout-60	--ldaptimeout 70	/ldaptimeout-80

See also /ldapipaddr, /ldapport, /ldapuser, /ldappwd, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapssl, and /ldapsslkey.

/ldapuser

Specifies the username that the POA can use to log in to the LDAP server in order to authenticate GroupWise client users. See "Providing LDAP Authentication for GroupWise Users" on page 461.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapuser-*LDAP_user_ID*	--ldapuser *LDAP_user_ID*	/ldapuser-*LDAP_user_ID*
Example:	/ldapuser-GWAuth	--ldapuser GWAuth	/ldapuser-GWAuth

See also /ldapipaddr, /ldapport, /ldappwd, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapssl, and /ldapsslkey, and /ldaptimeout.

/ldapuserauthmethod

Specifies the LDAP user authentication method you want the POA to use when accessing an LDAP server. Valid settings are bind and compare. See "Providing LDAP Authentication for GroupWise Users" on page 461.

	NetWare POA	Linux POA	Windows POA
Syntax:	/ldapuserauthmethod-*method*	--ldapuserauthmethod *method*	/ldapuserauthmethod-*method*
Example:	/ldapuserauthmethod-bind	--ldapuserauthmethod bind	/ldapuserauthmethod-compare

See also /ldapuser, /ldapipaddr, /ldapport, /ldappwd, /ldapdisablepwdchg, /ldapssl, and /ldapsslkey, and /ldaptimeout.

/lockoutresetinterval

Specifies the length of time the user login is disabled after lockout. The default is 30 minutes; the minimum setting is 15; there is no maximum setting. The login can also be manually re-enabled in ConsoleOne in the GroupWise Account page of the User object. If /lockoutresetinterval is set to 0 (zero), the login must be re-enabled manually through ConsoleOne. See "Enabling Intruder Detection" on page 465.

	NetWare POA	Linux POA	Windows POA
Syntax:	/lockoutresetinterval-*minutes*	--lockoutresetinterval *minutes*	/lockoutresetinterval-*minutes*
Example:	/lockoutresetinterval-15	--lockoutresetinterval 60	/lockoutresetinterval-90

See also /intruderlockout, /incorrectloginattempts, and /attemptsresetinterval.

/log

Specifies the directory where the POA stores its log files. On NetWare and Windows, the default location is the *post_office*\wpcsout\ofs directory. On Linux, the default location is the /var/log/novell/groupwise/*post_office_name*.poa directory. See "Using POA Log Files" on page 497.

	NetWare POA	Linux POA	Windows POA
Syntax:	/log-[*svr*\][*vol*:]*dir* /log-\\*svr**vol**dir*	--log /*dir*	/log-[*drive*:]*dir* /log-\\*svr**sharename**dir*
Example:	/log-\agt\log /log-\\server2\mail:\agt\log /log-\\server2\mail\agt\log	--log /gwsystem/logs	/log-\agt\log /log-m:\agt\log /log-\\server2\c\mail\agt\log

Typically you would find multiple log files in the specified directory. The first 4 characters represent the date. The next 3 characters identify the agent. A three-digit extension allows for multiple log files created on the same day. For example, a log file named 0518poa.001 would indicate that it is a POA log file, created on May 18. If you restarted the POA on the same day, a new log file would be started, named 0518poa.002.

See also /loglevel, /logdiskoff, /logdays, and /logmax.

/logdays

Specifies how many days to keep POA log files on disk. The default is 7 days. See "Using POA Log Files" on page 497.

	NetWare POA	Linux POA	Windows POA
Syntax:	/logdays-*days*	--logdays *days*	/logdays-*days*
Example:	/logdays-5	--logdays 10	/logdays-14

See also /log, /loglevel, /logdiskoff, and /logmax.

/logdiskoff

Turns off disk logging for the POA so no information about the functioning of the POA is stored on disk. The default is for logging to be turned on. See "Using POA Log Files" on page 497.

	NetWare POA	Linux POA	Windows POA
Syntax:	/logdiskoff	--logdiskoff	/logdiskoff

See also /loglevel.

/loglevel

Controls the amount of information logged by the POA. Logged information is displayed in the log message box and written to the POA log file during the current agent session. The default is Normal, which displays only the essential information suitable for a smoothly running POA. Use Verbose to display the essential information, plus additional information helpful for troubleshooting. Verbose logging does not degrade POA performance, but log files saved to disk consume more disk space when verbose logging is in use. See "Using POA Log Files" on page 497.

	NetWare POA	Linux POA	Windows POA
Syntax:	/loglevel-*level*	--loglevel *level*	/loglevel-*level*
Example:	/loglevel-verbose	--loglevel verbose	/loglevel-verbose

See also /log, /logdiskoff, /logdays, and /logmax.

/logmax

Sets the maximum amount of disk space for all POA log files. When the specified disk space is consumed, the POA deletes existing log files, starting with the oldest. The default is 65536 KB. See "Using POA Log Files" on page 497.

	NetWare POA	Linux POA	Windows POA
Syntax:	/logmax-*kilobytes*	--logmax *kilobytes*	/logmax-*kilobytes*
Example:	/logmax-32000	--logmax 130000	/logmax-16000

See also /log, /loglevel, /logdiskoff, and /logdays.

/maxappconns

Sets the maximum number of application connections allowed between the POA and the GroupWise clients run by GroupWise users. The default maximum number of application connections is 2048. See "Adjusting the Number of Connections for Client/Server Processing" on page 508.

	NetWare POA	Linux POA	Windows POA
Syntax:	/maxappconns-*number*	--maxappconns *number*	/maxappconns-*number*
Example:	/maxappconns-3072	--maxappconns 4096	/maxappconns-5120

See also /maxphysconns.

/maxphysconns

Sets the maximum number of physical TCP/IP connections allowed between the POA and the GroupWise clients run by GroupWise users. The default maximum number of physical connections is 1024. See "Adjusting the Number of Connections for Client/Server Processing" on page 508.

	NetWare POA	Linux POA	Windows POA
Syntax:	/maxphysconns-*number*	--maxphysconns *number*	/maxphysconns-*number*
Example:	/maxphysconns-2048	--maxphysconns 4096	/maxphysconns-5120

See also /maxappconns.

/msgtranssl

Sets the availability of secure SSL communication between the POA and its MTA. Valid settings are enabled and disabled. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

	NetWare POA	Linux POA	Windows POA
Syntax:	/msgtranssl-*setting*	--msgtranssl *setting*	/msgtranssl-*setting*
Example:	/msgtranssl-enabled	--msgtranssl enabled	/msgtranssl-enabled

See also /certfile, /keyfile and /keypassword.

/mtpinipaddr

Specifies the network address of the server where the POA runs, as either an IP address or a DNS hostname. See "Using TCP/IP Links between the Post Office and the Domain" on page 443.

	NetWare POA	Linux POA	Windows POA
Syntax:	/mtpinipaddr-*network_addr*	--mtpinipaddr *network_addr*	/mtpinipaddr-*network_addr*
Example:	/mtpinipaddr-172.16.5.18	--mtpinipaddr 172.16.5.19	/mtpinipaddr-172.16.5.20
	/mtpinipaddr-server1	--mtpinipaddr server2	/mtpinipaddr-server3

See also /mtpinport, /mtpoutipaddr, /mtpoutport, /mtpsendmax, and /nomtp.

/mtpinport

Sets the message transfer port number the POA listens on for messages from the MTA. The default is 7101. See "Using TCP/IP Links between the Post Office and the Domain" on page 443.

	NetWare POA	Linux POA	Windows POA
Syntax:	/mtpinport-*port_number*	--mtpinport *port_number*	/mtpinport-*port_number*
Example:	/mtpinport-7201	--mtpinport 7202	/mtpinport-7203

See also /mtpinipaddr, /mtpoutipaddr, /mtpoutport, /mtpsendmax, and /nomtp.

/mtpoutipaddr

Specifies the network address of the server where the MTA for the domain runs, as either an IP address or a DNS hostname. See "Using TCP/IP Links between the Post Office and the Domain" on page 443.

	NetWare POA	Linux POA	Windows POA
Syntax:	/mtpoutipaddr-*network_address*	--mtpoutipaddr *network_address*	/mtpoutipaddr-*network_address*
Example:	/mtpoutipaddr-172.16.5.18	--mtpoutipaddr 172.16.5.19	/mtpoutipaddr-172.16.5.19
	/mtpoutipaddr-server2	--mtpoutipaddr server3	/mtpoutipaddr-server4

See also /mtpinipaddr, /mtpinport, /mtpoutport, /mtpsendmax, and /nomtp.

/mtpoutport

Specifies the message transfer port number the MTA listens on for messages from the POA. The default is 7100. See "Using TCP/IP Links between the Post Office and the Domain" on page 443.

	NetWare POA	Linux POA	Windows POA
Syntax:	/mtpoutport-*port_number*	--mtpoutport *port_number*	/mtpoutport-*port_number*
Example:	/mtpoutport-7200	--mtpoutport 7300	/mtpoutport-7400

See also /mtpinipaddr, /mtpinport, /mtpoutipaddr, /mtpsendmax, and /nomtp.

/mtpsendmax

Sets the maximum size in megabytes for messages being sent outside the post office. By default, messages of any size can be transferred to the MTA. See "Restricting Message Size between Post Offices" on page 455.

	NetWare POA	Linux POA	Windows POA
Syntax:	/mtpsendmax-*megabytes*	--mtpsendmax *megabytes*	/mtpsendmax-*megabytes*
Example:	/mtpsendmax-2	--mtpsendmax 4	/mtpsendmax-6

See also /mtpinipaddr, /mtpinport, /mtpoutipaddr, /mtpoutport, and /nomtp.

/name

Specifies the object name of the POA object in the post office. If you have multiple POAs configured for the same post office, you must use this switch to specify which POA configuration to use when the POA starts. Several useful configurations include multiple POAs for a single post office, as described in the following sections:

- "Configuring a Dedicated Client/Server POA" on page 510
- "Configuring a Dedicated Message File Processing POA" on page 513
- "Configuring a Dedicated Indexing POA" on page 516
- "Configuring a Dedicated Database Maintenance POA" on page 518

	NetWare POA	Linux POA	Windows POA
Syntax:	/name-*object_name*	--name *object_name*	/name-*object_name*
Example:	/name-POA2	--name POA2	/name-POA2

/noada

Disables the POA admin thread. For an explanation of the POA admin thread, see "POA Admin Thread Status Box" on page 478.

The POA admin thread must run for at least one POA for each post office. However, it can be disabled for POAs with specialized functioning where the database update and repair activities of the POA admin thread could interfere with other, more urgent processing.

	NetWare POA	Linux POA	Windows POA
Syntax:	/noada	--noada	/noada

Historical Note: In GroupWise 5.2 and earlier, a separate agent, the Administration Agent (ADA), handled the functions now consolidated into the POA admin thread. Hence the switch name, /noada.

/nocache

Disables database caching. The default is for caching to be turned on. Use this switch if you are running NFS or if your backup system cannot back up open files.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nocache	--nocache	/nocache

/noconfig

Ignores any configuration information provided for the POA in ConsoleOne and uses only settings from the POA startup file. The default is for the POA to use the information provided in ConsoleOne, overridden as needed by settings provided in the startup file or on the command line.

	NetWare POA	Linux POA	Windows POA
Syntax:	/noconfig	--noconfig	/noconfig

/noerrormail

Prevents problem files from being sent to the GroupWise administrator. The default is for error mail to be sent to the administrator. See "Notifying the GroupWise Administrator" on page 503.

	NetWare POA	Linux POA	Windows POA
Syntax:	/noerrormail	--noerrormail	/noerrormail

/nogwchk

Turns off Mailbox/Library Maintenance processing for the POA. The default is for the POA to perform Mailbox/Library Maintenance tasks requested from ConsoleOne and configured as POA scheduled events.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nogwchk	--nogwchk	/nogwchk

See also /gwchkthreads.

/nomf

Turns off all message file processing for the POA. The default is for the POA to process all message files.

Two specialized configurations that require turning off message files are described in "Configuring a Dedicated Client/Server POA" on page 510 and "Configuring a Dedicated Indexing POA" on page 516.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nomf	--nomf	/nomf

See also /nomfhigh and /nomflow.

/nomfhigh

Turns off processing high priority messages files (message queues 0 and 1). For information about message queues, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nomfhigh	--nomfhigh	/nomfhigh

See also /nomf and /nomflow.

/nomflow

Turns off processing lower priority messages files (message queues 2 through 7). For information about message queues, see "Post Office Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nomflow	--nomflow	/nomflow

See also /nomf and /nomfhigh.

/nomtp

Disables Message Transfer Protocol, so that a TCP/IP link cannot be used between the POA and the MTA. See "Changing the Link Protocol between the Post Office and the Domain" on page 442.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nomtp	--nomtp	/nomtp

See also /mtpinipaddr, /mtpinport, /mtpoutipaddr, /mtpoutport, and /mtpsendmax.

/nonuu

Disables nightly user upkeep. See “Performing Nightly User Upkeep” on page 472.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nonuu	--nonuu	/nonuu

See also /nuuoffset.

/noqf

Disables the periodic QuickFinder™ indexing done by the POA. The default is for periodic indexing to be turned on. See “Regulating Indexing” on page 514.

	NetWare POA	Linux POA	Windows POA
Syntax:	/noqf	--noqf	/noqf

See also /qfinterval, /qfintervalinminute, /qfbaseoffset, and /qfbaseoffsetinminute.

/nordab

Disables daily generation of the system Address Book for Remote users. See “Performing Nightly User Upkeep” on page 472.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nordab	--nordab	/nordab

See also /rdaboffset.

/norecover

Disables automatic database recovery. The default is for automatic database recovery to be turned on.

If the POA detects a problem with a database, when automatic database recovery has been turned off, the POA notifies the administrator, but it does not recover the problem database. The administrator can then recover or rebuild the database as needed. See Chapter 26, “Maintaining Domain and Post Office Databases,” on page 345.

Two specialized configurations that require turning off automatic database recovery are described in “Configuring a Dedicated Client/Server POA” on page 510 and “Configuring a Dedicated Indexing POA” on page 516.

	NetWare POA	Linux POA	Windows POA
Syntax:	/norecover	--norecover	/norecover

/nosnmp

Disables SNMP for the POA. The default is to have SNMP enabled. See "Using SNMP Monitoring Programs" on page 499.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nosnmp	--nosnmp	/nosnmp

/notcpip

Disables TCP/IP communication for the POA. The default is to have TCP/IP communication enabled. Use this switch if you do not want this POA to communicate with GroupWise clients using TCP/IP.

	NetWare POA	Linux POA	Windows POA
Syntax:	/notcpip	--notcpip	/notcpip

Two specialized configurations that require turning off automatic database recovery are described in "Configuring a Dedicated Message File Processing POA" on page 513 and "Configuring a Dedicated Indexing POA" on page 516.

/nuuoffset

Specifies the number of hours after midnight for the POA to start performing user upkeep. The default is 1 hour; valid values range from 0 to 23. See "Performing Nightly User Upkeep" on page 472.

	NetWare POA	Linux POA	Windows POA
Syntax:	/nuuoffset-*hours*	--nuuoffset *hours*	/nuuoffset-*hours*
Example:	/nuuoffset-2	--nuuoffset 3	/nuuoffset-4

See also /nonuu.

/password

Provides the password for the POA to use when accessing post offices or document storage areas on remote servers. You can also provide user and password information on the Post Office Settings page in ConsoleOne. See "Starting the POA" on page 431.

	NetWare POA	Linux POA	Windows POA
Syntax:	/password-*NetWare_password*	--password *network_password*	/password-*network_password*
Example:	/password-GWise	--password GWise	/password-GWise

See also /user and /dn.

/port

Sets the TCP port number used for the POA to communicate with GroupWise clients in client/server access mode. The default is 1677. See "Using Client/Server Access to the Post Office" on page 447.

	NetWare POA	Linux POA	Windows POA
Syntax:	/port-*port_number*	--port *port_number*	/port-*port_number*
Example:	/port-1678	--port 1679	/port-1680

See also /ip.

/primingmax

Sets the maximum number of TCP handler threads that POA can use for priming users' Caching mailboxes. The default is 20 per cent. See "Supporting Forced Mailbox Caching" on page 454.

	NetWare POA	Linux POA	Windows POA
Syntax:	/primingmax-*percentage*	--primingmax *percentage*	/primingmax-*percentage*
Example:	/primingmax-40	--primingmax 50	/primingmax-60

See also /tcpthreads.

/qfbaseoffset

Specifies the number of hours after midnight for the POA to start its indexing cycle as specified by the /qfinterval or /qfintervalinminute switch. The default is 20 hours (meaning at 8:00 p.m.); valid values range from 0 to 23. See "Regulating Indexing" on page 514.

	NetWare POA	Linux POA	Windows POA
Syntax:	/qfbaseoffset-*hours*	--qfbaseoffset *hours*	/qfbaseoffset-*hours*
Example:	/qfbaseoffset-1	--qfbaseoffset 2	/qfbaseoffset-3

See also /qfbaseoffsetinminute, /qfinterval, /qfintervalinminute, and /noqf.

/qfbaseoffsetinminute

Specifies the number of minutes after midnight for the POA to start its indexing cycle as specified by the /qfinterval or /qfintervalinminute switch. The default is 20 hours (1200 minutes, meaning at 8:00 p.m.). The maximum setting is 1440 (24 hours). See "Regulating Indexing" on page 514.

	NetWare POA	Linux POA	Windows POA
Syntax:	/qfbaseoffsetinminute-*minutes*	--qfbaseoffsetinminute *minutes*	/qfbaseoffsetinminute-*minutes*

	NetWare POA	Linux POA	Windows POA
Example:	/qfbaseoffset-30	--qfbaseoffset 45	/qfbaseoffset-90

See also /qfbaseoffset, /qfinterval, /qfintervalinminute, and /noqf.

/qfinterval

Specifies the interval in hours for the POA to update the QuickFinder indexes in the post office. The default is 24 hours. See "Regulating Indexing" on page 514.

	NetWare POA	Linux POA	Windows POA
Syntax:	/qfinterval-*hours*	--qfinterval-*hours*	/qfinterval-*hours*
Example:	/qfinterval-12	--qfinterval-6	/qfinterval-2

See also /qfbaseoffset, /qfbaseoffsetinminute, /qfintervalinminute, and /noqf.

/qfintervalinminute

Specifies the interval in minutes for the POA to update the QuickFinder indexes in the post office. The default is 24 hours (1440 minutes). See "Regulating Indexing" on page 514.

	NetWare POA	Linux POA	Windows POA
Syntax:	/qfintervalinminute-*minutes*	--qfintervalinminute *minutes*	/qfintervalinminute-*minutes*
Example:	/qfintervalinminute-90	--qfintervalinminute 30	/qfintervalinminute-120

See also /qfinterval, /qfbaseoffset, /qfbaseoffsetinminute, and /noqf.

/rdaboffset

Specifies the number of hours after midnight for the POA to generate the daily copy of the system Address Book for Remote users. The default is 0; valid values range from 0 to 23. See "Performing Nightly User Upkeep" on page 472.

	NetWare POA	Linux POA	Windows POA
Syntax:	/rdaboffset-*hours*	--rdaboffset *hours*	/rdaboffset-*hours*
Example:	/rdaboffset-2	--rdaboffset 3	/rdaboffset-4

See also /nordab.

/rights

Verifies that the POA has the required network rights or permissions to all directories where it needs access in the post office directory.

When started with this switch, the POA lists directories it is checking, which can be a lengthy process. Use this switch on an as needed basis, not in the POA startup file. If the POA encounters inadequate rights or permissions, it indicates the problem and shuts down.

	NetWare POA	Linux POA	Windows POA
Syntax:	/rights	--rights	/rights

/sleep

Sets how long NetWare POA threads remain dormant when the CPU utilization threshold has been exceeded. The default is 100 milliseconds. See "Optimizing CPU Utilization for the NetWare POA" on page 520.

	NetWare POA	Linux POA	Windows POA
Syntax:	/sleep-*milliseconds*	N/A	N/A
Example:	/sleep-300	N/A	N/A

See also /cpu.

/tcpthreads

Specifies the maximum number of TCP handler threads the POA can create to service client/server requests. The default is 6; valid values range from 1 to 99. Plan on about one TCP handler thread per 20-30 client/server users. See "Adjusting the Number of POA Threads for Client/Server Processing" on page 507.

	NetWare POA	Linux POA	Windows POA
Syntax:	/tcpthreads-*number*	--tcpthreads *number*	/tcpthreads-*number*
Example:	/tcpthreads-10	--tcpthreads 20	/tcpthreads-20

See also /primingmax.

/threads

Specifies the maximum number of message handler threads the POA can create. The default is 8; valid values range from 1 to 30. See "Adjusting the Number of POA Threads for Message File Processing" on page 512.

	NetWare POA	Linux POA	Windows POA
Syntax:	/threads-*number*	--threads *number*	/threads-*number*
Example:	/threads-10	--threads 20	/threads-30

/user

Provides the network user ID for the POA to use when accessing post offices and/or document storage areas on remote servers. You can also provide user and password information on the Post Office Settings page in ConsoleOne. For the NetWare POA, see "Creating a NetWare Account for Agent Access (Optional)" in "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

	NetWare POA	Linux POA	Windows POA
Syntax:	/user-*eDirectory_user_ID*	--user *Linux_user_ID*	/user-*Windows_user_ID*
Example:	/user-GWAgents	--user GWAgents	/user-GWAgents

See also /password and /dn.

NetWare Note: The *eDirectory_user_ID* is a user that the POA can use to log in to the remote NetWare server.

Linux Note: On OES Linux, the *Linux_user_ID* is a LUM-enabled user that the POA can use to log in to the remote OES Linux server. On SLES Linux, it is a standard Linux user.

Windows Note: The *Windows_user_ID* is a user that the POA can use to log in to the remote Windows server. The Windows POA gains access to the post office directory when it starts. However, a particular user might attempt to access a remote document storage area to which the POA does not yet have a drive mapping available. By default, the POA attempts to map a drive using the same user ID and password it used to access the post office directory. If the user ID and password for the remote storage area are different from the post office, then use the /user and /password switches to specify the needed user ID and password. You can also provide user and password information on the Post Office Settings page in ConsoleOne. However, it is preferable to use the same user ID and password on all servers where the POA needs access.

X

Message Transfer Agent

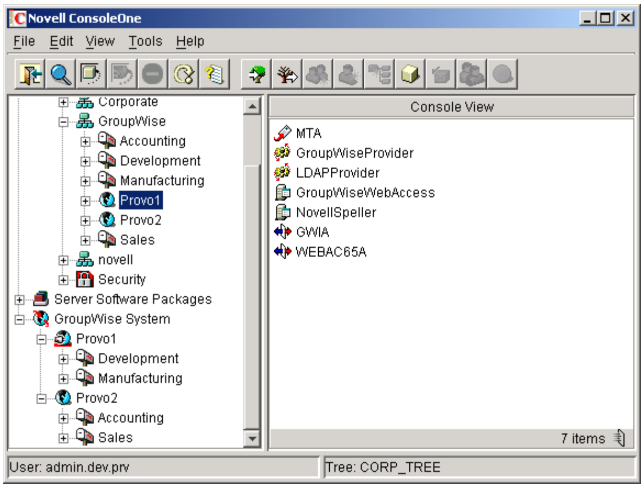
41 Understanding Message Transfer between Domains and Post Offices

A domain organizes post offices into a logical grouping for addressing, routing, and administration purposes in your GroupWise® system. Messages are transferred between post offices and domains by the Message Transfer Agent (MTA). The following topics help you understand domains and the functions of the MTA:

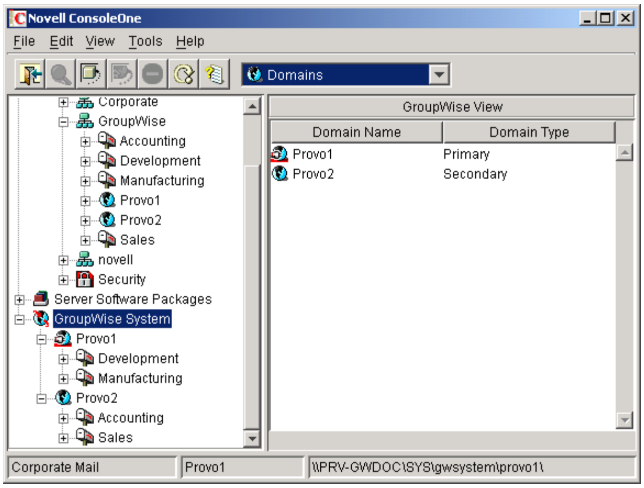
- "Domain Representation in ConsoleOne" on page 557
- "Domain Directory Structure" on page 558
- "Information Stored in the Domain" on page 558
- "Role of the Message Transfer Agent" on page 559
- "Link Configuration between Domains and Post Offices" on page 560
- "Message Flow between Domains and Post Offices" on page 560
- "Cross-Platform Issues between Domains and Post Offices" on page 561

Domain Representation in ConsoleOne

In ConsoleOne®, domains are container objects that contain an MTA object, as well as other domain-related objects, as shown below:



Although each post office is linked to a domain, it does not display as subordinate to the domain in the Console View. However, using the GroupWise View, you can display post offices as subordinate to the domains to which they are linked in your GroupWise system.



Domain Name	Domain Type
Provo1	Primary
Provo2	Secondary

Corporate Mail | Provo1 | \\PRV-GWDOC\SYS\gwsystem\provo1\

Domain Directory Structure

Physically, a domain consists of a set of directories that house all the information stored in the domain. See "Domain Directory" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Information Stored in the Domain

The following types of information are stored in the domain:

- "Domain Database" on page 558
- "Agent Input/Output Queues in the Domain" on page 559
- "Gateways" on page 559

No messages are stored in the domain, so GroupWise client users do not need access to the domain directory. The only person who needs file access to the domain directory is the GroupWise administrator.

Domain Database

The domain database (wpdomain.db) contains all administrative information for the domain, including:

- Address information about all GroupWise objects (such as users, resources, post offices, and gateways in the domain)
- System configuration and linking information for the domain's MTA
- Address and message routing information to other domains

The first domain you create is the primary domain. In the primary domain, the wpdomain.db file contains all administrative information for your entire GroupWise system (all its domains, post offices, users, and so on). Because the wpdomain.db file in the primary domain is so crucial, you should back it up regularly and keep it secure. See "Backing Up a Domain" on page 375.

You can re-create your entire GroupWise system from the primary domain wpdomain.db file; however, if the primary domain wpdomain.db file becomes unusable, you can no longer make administrative updates to your GroupWise system.

In a secondary domain, the wpdomain.db file contains administrative information about that secondary domain only.

Agent Input/Output Queues in the Domain

Each domain contains agent input/output queues where messages are deposited and picked up for processing by the MTA.

For a mapped or UNC link between domains, the MTA requires read/write access rights to its input/output queues in the other domains. For a TCP/IP link, no access rights are required because messages are communicated by way of TCP/IP.

For illustrations of the processes presented below, see "Message Flow between Domains and Post Offices" on page 560.

MTA Input Queue in the Domain

The MTA input queue in the local domain (*domain*\wpcsin) is where MTAs for other domains deposit user messages for the local MTA to route to local post offices or to route to other domains. Thus the MTA input queue in the local domain is the output queue for the MTAs in many other domains.

The MTA does not have an output queue for user messages in the local domain. Because its primary task is routing messages, the local MTA has output queues in all post offices in the domain. See "POA Input Queue in the Post Office" on page 421. The local MTA also has output queues in all domains to which it is directly linked.

MTA Output Queue in the Domain

The MTA output queue in the local domain (*domain*\wpcsout\ads) is where the MTA deposits administrative messages from other domains for the MTA admin thread to pick up.

MTA Admin Thread Input Queue in the Domain

The MTA admin thread input queue (*domain*\wpcsout\ads) is, of course, the same as the MTA output queue in the local domain. The MTA admin thread picks up administrative messages deposited in the queue by the MTA and updates the domain database.

MTA Admin Thread Output Queue in the Domain

The MTA admin thread output queue (*domain*\wpcsin) is the same as the MTA input queue in the local domain. The MTA admin thread deposits administrative messages in the queue for replication to other domains.

Gateways

Gateways are installed and configured at the domain level of your GroupWise system. For a list of gateways, see GroupWise 6.*x* Gateways (http://www.novell.com/documentation/gw6xgate/index.html). GroupWise 5.5 gateways can be used with GroupWise 6.5.

Role of the Message Transfer Agent

You must run an MTA for each domain. The MTA:

- Routes messages between post offices in the local domain.
- Routes messages between domains.
- Routes messages to and from gateways installed in the local domain.

- Routes messages between GroupWise systems across the Internet if appropriate DNS lookup capabilities have been set up. See "Using Dynamic Internet Links" in "Connecting to GroupWise 5.x and 6.x Systems" in the *GroupWise 6.5 Multi-System Administration Guide*.
- Schedules routing of messages across expensive links. See "Scheduling Direct Domain Links" on page 593.
- Controls the size of messages that can pass across links. See "Restricting Message Size between Domains" on page 588.
- Updates the domain database (wpdomain.db) whenever GroupWise users, resources, post offices, or other GroupWise objects are added, modified, or deleted.
- Replicates updates to all domains and post offices throughout your GroupWise system. This keeps the Address Book up to date for all GroupWise users.
- Synchronizes GroupWise user information with Novell® eDirectory™ user information. This handles updates made in ConsoleOne without the GroupWise Administrator snap-in running. See "Using eDirectory User Synchronization" on page 598.
- Synchronizes GroupWise object information throughout your GroupWise system as needed.
- Detects and repairs invalid information in the domain database (wpdomain.db).
- Provides improved performance for GroupWise Remote client users. See "Enabling Live Remote" on page 589.
- Provides logging and statistics about GroupWise message flow. See "Enabling MTA Message Logging" on page 603.

Link Configuration between Domains and Post Offices

In GroupWise, a link is defined as the information required to route messages between domains, post offices, and gateways in a GroupWise system. Links are created and configured when new domains, post offices, and gateways are created.

For more specific information about how domains are linked to each other, and about how domains and post offices are linked, see Chapter 10, "Managing the Links between Domains and Post Offices," on page 131.

Message Flow between Domains and Post Offices

When messages travel beyond the local post office, a variety of link configuration alternatives are possible.

- "Message Flow between Post Offices in the Same Domain" on page 560
- "Message Flow between Different Domains" on page 561

Message Flow between Post Offices in the Same Domain

To compare the types of links between a domain and its post offices and to see what happens to message flow within the domain when the domain is closed, view the following message flow diagrams:

- "TCP/IP Link Open: Transfer between Post Offices Successful"
- "TCP/IP Link Closed: Transfer between Post Offices Delayed"

- "Mapped/UNC Link Open: Transfer between Post Offices Successful"
- "Mapped/UNC Link Closed: Transfer between Post Offices Delayed"

All of these diagrams are found in "Message Delivery to a Different Post Office" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Message Flow between Different Domains

To compare mapped and UNC links with TCP/IP links and to see what happens to message flow when the destination domain is closed, view the following message flow diagrams:

- "TCP/IP Link Open: Transfer between Domains Successful"
- "TCP/IP Link Closed: Transfer between Domains Delayed"
- "Mapped/UNC Link Open: Transfer between Domains Successful"
- "Mapped/UNC Link Closed: Transfer between Domains Delayed"

All of these diagrams are found in "Message Delivery to a Different Domain" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Cross-Platform Issues between Domains and Post Offices

Domains can be located on the following platforms:

- Novell NetWare®
- Windows NT/2000
- Linux (GroupWise 6.5 for Linux)
- UNIX (GroupWise 5.*x*)

The GroupWise agents can run on the following platforms:

- Novell NetWare
- Windows NT/2000
- Linux (GroupWise 6.5 for Linux)
- UNIX (GroupWise 5.*x*)

In general, GroupWise is most efficient if you match the agent platform with the network operating system. Ideally, the MTA as well as the domain and post offices should be on the same platform. However, those with mixed networks may wonder what combinations are possible. You have several alternatives.

- "MTA Platform Dependencies Because of Direct Access Requirements to Post Offices" on page 562
- "MTA/Post Office Platform Independence through TCP/IP Links" on page 562
- "MTA Platform Dependencies Because of Direct Access Requirements to the Domain" on page 562
- "MTA/Domain Platform Independence through TCP/IP Links" on page 563
- "MTA/Domain Platform Independence through the Transfer Pull Configuration" on page 563

MTA Platform Dependencies Because of Direct Access Requirements to Post Offices

The MTA must always have direct access to the domain directory. In addition, if using mapped or UNC links to post offices, the MTA must have direct access to each post office directory as well. If the MTA is installed on a remote server, it must be able to log in to servers where the post offices are located.

The table below summarizes the various combinations of MTA and post office platforms, and indicates which combinations work for direct access and which ones do not:

	NetWare MTA	Windows MTA	Linux MTA	UNIX MTA
Post Office on NetWare	Yes	Yes	No[3]	Not supported[2]
Post Office on Windows	No[1]	Yes	No[3]	Not supported[2]
Post Office on Linux	No[3]	No[3]	No[3]	No[3]
Post Office on UNIX	Not supported[2]	Not supported[2]	No[3]	Supported for GroupWise 5.*x*
Post Office on Macintosh	No[4]	No[4]	No[4]	No[4]

[1] The NetWare® MTA cannot service a domain or post office on a Windows server because Windows does not support the required cross-platform connection.

[2] For these combinations, an NFS connection would be required, which is not a supported configuration for the agents. However, the agents often can work adequately in this configuration.

[3] TCP/IP links are required between the MTA and the POA in GroupWise 6.5 for Linux. Direct access to post offices is not available.

[4] Domains and post offices cannot be created on Macintosh computers.

MTA/Post Office Platform Independence through TCP/IP Links

To overcome platform dependencies for post offices, create a TCP/IP link for any post office located on a platform where the domain MTA cannot gain direct access. See "Using TCP/IP Links between a Domain and its Post Offices" on page 583.

MTA Platform Dependencies Because of Direct Access Requirements to the Domain

If using mapped or UNC links between domains, the source domain MTA must have direct access to its input queues in the destination domain directory. If the MTA is installed on a remote server, it must be able to log in to the server where its domain located.

The table below summarizes the various combinations of the platform of MTA for the source domain and the platform where the destination domain is located, and indicates which combinations work for direct access and which ones do not:

	NetWare MTA for Source Domain	Windows MTA for Source Domain	Linux MTA for Source Domain	UNIX MTA for Source Domain
Destination Domain on NetWare	Yes	Yes	No[3]	Not supported[2]
Destination Domain on Windows	No[1]	Yes	No[3]	Not supported[2]
Destination Domain on Linux	No[3]	No[3]	No[3]	No[3]
Destination Domain on UNIX	Not supported[2]	Not supported[2]	No[3]	Supported with GroupWise 5.*x*
Destination Domain on Macintosh	No[4]	No[4]	No[4]	No[4]

[1] The NetWare MTA cannot write message files into its output queue in a destination domain on a Windows server because Windows does not support the required cross-platform connection.

[2] For these combinations, an NFS connection would be required, which is not a supported configuration for the agents.

[3] TCP/IP links are required between MTAs in GroupWise 6.5 for Linux. Direct access to other domains is not available.

[4] Domains cannot be created on Macintosh computers.

MTA/Domain Platform Independence through TCP/IP Links

To overcome platform dependencies between domains, use TCP/IP links between domains. See "Using TCP/IP Links between Domains" on page 579.

MTA/Domain Platform Independence through the Transfer Pull Configuration

If TCP/IP is not available, another alternative for overcoming platform dependencies is a transfer pull configuration.

By default the MTA "pushes" message files out to destination domains by writing them into its output queue in each destination domain. One situation where this method will not work is for the NetWare MTA on a NetWare server to write message files to its input queue in a destination domain located on a Windows server.

As an alternative, you can have the Windows MTA for the destination domain "pull" the message files from the source domain on the NetWare server. This is called a transfer pull configuration. See "Using a Transfer Pull Configuration" on page 596 for setup instructions. See also "Alternate Link Configuration: Transfer Pull" in "Message Delivery to a Different Domain" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

42 Installing and Starting the MTA

Detailed instructions for installing and starting the MTA for the first domain of a new GroupWise® system are provided in "Installing a Basic GroupWise System" in the *GroupWise 6.5 Installation Guide*. Additional agent installation and startup instructions and worksheets are available in "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

IMPORTANT: If you are installing and running the MTA in a clustered GroupWise system, see the appropriate section of the GroupWise 6.5 Interoperability Guide before you install the MTA:

- "Deciding How to Install and Configure the Agents in a Cluster" in "Novell Cluster Services"
- "Deciding How to Install and Configure the Agents in a Cluster" in "Microsoft Clustering Services"

This section presents some additional MTA installation and startup information that may be useful as you install and start additional MTAs throughout your GroupWise system.

- "Installing the MTA Software" on page 565
- "Starting the MTA" on page 568
- "Uninstalling the MTA Software" on page 573

Installing the MTA Software

Select the platform where you have installed the MTA:

- "Fine-Tuning Your NetWare MTA Installation" on page 565
- "Fine-Tuning Your Linux MTA Installation" on page 567
- "Fine-Tuning Your Windows MTA Installation" on page 567

Fine-Tuning Your NetWare MTA Installation

After initial installation, you can fine-tune your NetWare® MTA installation for improved performance:

- "Recommended NetWare Server Parameters for the NetWare MTA" on page 565
- "Estimating NetWare MTA Memory Requirements" on page 566

Recommended NetWare Server Parameters for the NetWare MTA

The default Maximum Packet Receive Buffers setting on a NetWare server is inadequate for the NetWare MTA in configurations that include numerous TCP/IP and remote file connections. Set Maximum Packet Receive Buffers to at least 2500 for the NetWare MTA in such configurations.

If you are also running the NetWare POA on the same server, see "Recommended NetWare Server Parameters for the NetWare POA" on page 427.

Estimating NetWare MTA Memory Requirements

The amount of memory required for the NetWare MTA is influenced by many factors, including:

- Number of post offices and domains
- Volume of message traffic between post offices and domains
- Volume of large messages (for example, large attachments, remote updates, and so on)
- TCP/IP or mapped/UNC links between MTAs

The table below provides approximate memory requirements for various MTA activities. Actual numbers may vary somewhat from release to release, but the numbers provided do illustrate what activities require relatively more or less memory and what configuration options require more memory than others. This information can be used to produce a rough estimate of the memory required for your particular MTA configuration. Always remember this basic rule when it comes to planning for memory: More is better.

MTA Component	Approx. Memory	References
Agent Engine (gwenn4.nlm)[1]	5500 KB	(required)
MTA (gwmta.nlm)	469 KB	(required)
Main thread, UI, CSS, logging, statistics	140 KB	(required)
Dispatcher thread	500 KB	(required)
Scanner threads (each)[2]	40 KB	(required) See "Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices" on page 638. See also /fast0 and /fast4.
Router threads (each)	40 KB	(required) See "Optimizing the Routing Queue" on page 639. See also /maxrouters and /maxidlerouters.
Routing queue Queue entry size Queue base size	 60 KB 1920 KB	(required)
Direct connections (1 per domain/post office)	10 KB	(required for direct connections) See "Using Mapped or UNC Links between Domains" on page 582.
TCP master receiver	200 KB	(required for TCP/IP connections) See "Using TCP/IP Links between Domains" on page 579. See also /tcpport.

MTA Component	Approx. Memory	References
IP sender threads (each)	15 KB	1 required for TCP/IP connections; up to 4 available)
IP receiver threads (each)[3]	15 KB	(required for TCP/IP connections) See "Adjusting the Number of MTA TCP/IP Connections" on page 635. See also /tcpinbound.
Admin thread Idle Processing	 20 KB 125 KB	(required for domain database update and repair) See "Displaying MTA Admin Thread Status" on page 613. See also /noada.
eDirectory user synchronization (when active)	35 KB	(required for eDirectory user synchronization) See "Using eDirectory User Synchronization" on page 598. See also /nondssync.

[1] The Agent Engine (gwenn4.nlm) needs to be loaded only once per server, no matter how many agents (POAs and/or MTAs) are running on that server, as long as they are running in the same address space.

[2] By default, there are 2 scanner threads, for a default total of 80 KB. For TCP/IP connections, additional scanner threads are created for each location to which the MTA connects.

[3] By default, there are 40 receiver threads, for a default total of 600 KB for inbound connections.

The table below provides some very general memory figures for running both GroupWise agents on the same server.

Concurrent Users	Actual Memory Usage at Peak Time
100 active users (100-250 users in post office)	50 MB
250 active users (250-500 users in post office)	110 MB
500 active users (500-1000 users in post office)	125 MB
1000 active users (1000-2500 users in post office)	150 MB

Fine-Tuning Your Linux MTA Installation

After initial installation on Linux, no fine-tuning is necessary. The MTA runs very efficiently in a standard Linux installation.

Fine-Tuning Your Windows MTA Installation

After initial installation, you can fine-tune your Windows MTA installation for improved performance:

- "Recommended Windows Parameters for the Windows MTA" on page 568
- "Estimating Windows MTA Memory Requirements" on page 568

Recommended Windows Parameters for the Windows MTA

If you are running the Windows MTA for a domain or post offices located on a NetWare server, you might need to increase Maximum File Locks Per Connection from its default setting.

Estimating Windows MTA Memory Requirements

Although the Windows MTA memory requirements differ slightly from the NetWare MTA, you can use the figures provided for the NetWare MTA to see what MTA processes are most memory intensive. See "Estimating NetWare MTA Memory Requirements" on page 566.

Starting the MTA

Select the platform where you are starting the MTA:

- "Starting the NetWare MTA" on page 568
- "Starting the Linux MTA" on page 570
- "Starting the Windows MTA" on page 571

Starting the NetWare MTA

You can start the NetWare MTA in several ways:

- "Manually on the Command Line" on page 568
- "With a Startup File" on page 569
- "Automatically in the autoexec.ncf File" on page 570

Manually on the Command Line

To start a new NetWare MTA on the command line:

1 Go to the console of the NetWare server where the NetWare MTA is installed.

or

Use Remote Console to access the server:

1a Press Al+F1 to display the options.

1b Choose Select a Screen to View.

1c Choose System Console.

2 Enter the command to load the MTA NLM.

Syntax: `load gwmta.nlm /home [`*`svr`*`\][`*`vol`*`:]\`*`domain_dir`*

Example:

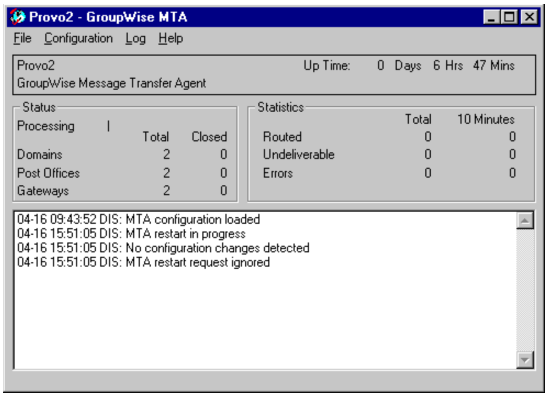
```
load gwmta.nlm /home-server2\mail:\provo2
```

The /home startup switch is required to start the NetWare MTA.

If the domain or post offices are located on different servers from where the NetWare MTA is running, the /dn switch or the /user and /password switches are also required so the NetWare MTA can log in to those servers. For an alternative to direct access for post offices, see "Using TCP/IP Links between a Domain and its Post Offices" on page 583.

If the domain is located on a different server from where the NetWare MTA is running, use the /work switch to specify a local directory for the MTA holding queues. The default location is the domain directory, which is not appropriate when the domain is located on a different server from where the NetWare MTA is running.

The NetWare MTA agent console will appear and display normal startup status messages. See Chapter 44, “Monitoring the MTA,” on page 605.



Provo2 Up Time: 0 Days 6 Hrs 47 Mins
GroupWise Message Transfer Agent

Status

Processing |

	Total	Closed
Domains	2	0
Post Offices	2	0
Gateways	2	0

Statistics

	Total	10 Minutes
Routed	0	0
Undeliverable	0	0
Errors	0	0

```
04-16 09:43:52 DIS: MTA configuration loaded
04-16 15:51:05 DIS: MTA restart in progress
04-16 15:51:05 DIS: No configuration changes detected
04-16 15:51:05 DIS: MTA restart request ignored
```

If the NetWare MTA agent console does not appear, see “Message Transfer Agent Problems” in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

When you start the NetWare MTA as described above, it is configured according to the MTA settings specified in ConsoleOne®. You can go to ConsoleOne and modify MTA functioning as needed. See “Configuring the MTA in ConsoleOne” on page 577.

With a Startup File

Another way to start the NetWare MTA is to use a startup file. You could use a startup file with the NetWare MTA for the following reasons:

- Overriding MTA settings defined in ConsoleOne
- Controlling the MTA locally without using ConsoleOne
- Adjusting specialized MTA functions that are not controllable from ConsoleOne

When you run the Agent Installation program, an initial MTA startup file is created in the agent installation directory. It is named using the first 8 characters of the domain name with a .mta extension. This initial startup file includes the /home startup switch set to the location of the domain directory.

If the domain or any or its post offices are located on a different server from where the NetWare MTA is running, you must edit the startup file and provide settings for the /user and /password switches so the NetWare MTA can log in to those servers. For an alternative to direct access for post offices, see “Using TCP/IP Links between a Domain and its Post Offices” on page 583. For an alternative to direct access for other domains, see “Using TCP/IP Links between Domains” on page 579.

If the domain serviced by the NetWare MTA is located on a different server from where the NetWare MTA is running, use the /work switch to specify a local directory for the MTA holding queues. The default location is the domain directory, which is not appropriate when the domain is located on a different server from where the NetWare MTA is running.

The MTA startup file can be modified to use other startup switches as needed. Startup switches specified on the command line override those in the startup file. Startup switches in the startup file override corresponding settings in ConsoleOne. See Chapter 46, "Using MTA Startup Switches," on page 643.

When you use a startup file, you must include it on the command line when you load the NetWare MTA. For example:

Syntax: `load gwmta.nlm @MTA_startup_file`

Example: `load gwmta.nlm @provo2.mta`

In addition to the initial MTA startup file, the Agent Installation program also provides a grpwise.ncf file to load the agents. If you will run only the NetWare MTA, you should edit the grpwise.ncf file to remove the command to load the POA.

Automatically in the autoexec.ncf File

After the NetWare MTA is running smoothly, you should modify the NetWare startup file, autoexec.ncf, to load the NetWare MTA and required NLM programs automatically whenever you restart the server

IMPORTANT: If you are running the MTA in a Novell cluster, see "Configuring the GroupWise Volume Resource to Load and Unload the Agents" in "Novell Cluster Services" in the *GroupWise 6.5 Interoperability Guide* for alternative instructions.

1. Edit the autoexec.ncf file in the NetWare sys:\system directory.
2. Add the following command to load the agents:

   ```
   grpwise.ncf
   ```

   or

   To start the agents in protected mode, add the following command:

   ```
   protect grpwise.ncf
   ```

3. Save the autoexec.ncf file.
4. If possible, restart the server to verify that the NLM programs and the NetWare MTA are loading properly.

Starting the Linux MTA

You can start the Linux MTA in several ways:

- "Manually with a User Interface" on page 570
- "Manually As a Daemon" on page 571
- "Automatically at System Startup" on page 571

Manually with a User Interface

1. Make sure you are logged in as root.
2. Change to the GroupWise agent bin directory.

   ```
   cd /opt/novell/groupwise/agents/bin
   ```

3. Enter the following command to start the MTA:

Syntax:

```
./gwmta --show --home domain_directory &
```

Example:

```
./gwmta --show --home /gwsystem/domlnx &
```

The MTA startup file is created by the Installation Advisor in the /opt/novell/groupwise/agents/share directory and is named after the domain that the MTA services. Because the Installation Advisor prompted you for the domain name and directory, it can set the --home startup switch in the MTA startup file. In the bin directory where the MTA executable is located, you could start the MTA with a command similar to the following example:

```
./gwmta --show @../share/lnxdom.poa
```

Manually As a Daemon

1 Make sure you are logged in as root.

2 Change to the /etc/init.d directory.

3 To start the Linux MTA (and perhaps the POA as well, depending on the configuration of the server), enter the following command:

```
./grpwise start
```

4 To confirm that the agents have started, enter the following command:

```
ps -eaf | grep gw
```

This lists all GroupWise agent process IDs.

Automatically at System Startup

If you selected Launch GroupWise Agents on System Startup in the Agent Installation program, the Agent Installation program configured your system so that the agents would start automatically each time you restart your server. The Agent Installation program always creates a grpwise startup script in /etc/init.d for starting the agents. To enable automatic startup, the Agent Installation program also creates symbolic links named S99grpwise in the rc3.d and rc5.d directories so that the agents load on restart into level 3 or 5, depending on the configuration of your Linux system.

When the grpwise script runs and starts the agents, it reads the agent startup files in /opt/novell/groupwise/agents/share to check for configuration information provided by startup switches. Because the --show switch cannot be used in the startup files, the agents never run with agent console interfaces when started automatically when the server restarts.

During agent installation, if you specified only a domain and no post offices, only an MTA startup file was created and the grpwise startup script starts only the MTA.

Starting the Windows MTA

You can start the Windows MTA in several ways:

- "Manually from the Windows Desktop" on page 572
- "With a Startup File" on page 572
- "Automatically in the Windows Startup Group" on page 572
- "Automatically as a Windows Service" on page 572

Manually from the Windows Desktop

In Windows, click Start > Programs > GroupWise Agents, then start the Windows MTA.

The Windows MTA agent console should appear and display normal startup status messages. See Chapter 44, “Monitoring the MTA,” on page 605.

If the Windows MTA agent console does not appear, see “Message Transfer Agent Problems” in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

When you start the Windows MTA as described above, it is configured according to the MTA settings specified in ConsoleOne. You can go to ConsoleOne and modify MTA functioning as needed. See “Configuring the MTA in ConsoleOne” on page 577.

With a Startup File

Another way to start the Windows MTA is to use a startup file. You could use a startup file to configure the MTA for the following reasons:

- Overriding MTA settings defined in ConsoleOne
- Controlling the MTA locally without using ConsoleOne
- Adjusting specialized MTA functions that are not controllable from ConsoleOne

When you run the Agent Installation program, an initial MTA startup file is created in the agent installation directory. It is named using the first 8 characters of the domain name with a .mta extension. This initial startup file includes the /home startup switch set to the location of the domain directory.

The MTA startup file can be modified to use other startup switches as needed. Startup switches in the startup file override corresponding settings in ConsoleOne. See Chapter 46, “Using MTA Startup Switches,” on page 643.

Automatically in the Windows Startup Group

After the Windows MTA is running smoothly, you should add it to the Windows Startup group to start the Windows MTA automatically whenever you restart your Windows server.

1. In Windows NT, click Start > Settings > Taskbar > Start Menu Programs > Add.

   or

   In Windows 2000, click Start > Settings > Taskbar & Start Menu > Advanced > Add.
2. Browse to the directory where you installed the Windows MTA.
3. Double-click GWMTA.EXE, then add the startup file to the command line.

   Example: `gwmta.exe @provo2.mta`
4. Click Next.
5. Select the Startup folder, provide a name for the shortcut, then click Finish.
6. If possible, restart the server to verify that the Windows MTA starts when you log in.

Automatically as a Windows Service

To start the GroupWise Windows MTA as a service for the first time after installation:

1. From the Windows desktop, click Start > Settings > Control Panel.

2 Double-click Services, select the MTA service (named after the domain), then click Start.

To make sure the MTA starts automatically each time you restart the server:

1 Click Start > Settings > Control Panel.

2 Double-click Services, select the MTA service (named after the domain), then click Startup.

3 Select Automatic, then click OK.

Thereafter, you will be able to manage the Windows agents just as you would any other services.

Uninstalling the MTA Software

If you move the MTA to a different server, you can uninstall the POA software from the old location to regain disk space as long as the MTA is not running on the server. Select the platform where you have been running the MTA:

- "Uninstalling the NetWare or Windows MTA" on page 573
- "Uninstalling the Linux MTA" on page 573

Uninstalling the NetWare or Windows MTA

1 Stop the MTA.

2 Run install.exe in the \agents subdirectory of the GroupWise software distribution directory or *GroupWise 6.5 Administrator* CD.

3 In the Install/Uninstall dialog box, click Uninstall to remove the MTA software from the server.

Windows Note: If the Windows MTA was running as a service, the Agent Installation program removes the service, registry entry, and Start menu icon from Windows.

Uninstalling the Linux MTA

1 Make sure you are logged in as root.

2 Stop the MTA.

3 Enter the following command to determine the specific version of the MTA that is running on the server:

```
rpm -qa | grep groupwise
```

4 Enter the following command to uninstall the MTA:

```
rpm -e novell-groupwise-agents-version-date
```

where *version* is the version number (for example, 6.5.1) and *date* is the is the date when the agent RPM was created (for example, 0428 for April 28).

This process removes all files and directories associated with the MTA.

43 Configuring the MTA

As your GroupWise® system grows and evolves, you will probably need to modify MTA configuration to meet changing system needs. The following topics help you configure the MTA:

Performing Basic MTA Configuration

MTA configuration information is stored as properties of its MTA object in eDirectory. The following topics help you modify the MTA object in ConsoleOne and change MTA configuration to meet changing system configurations:

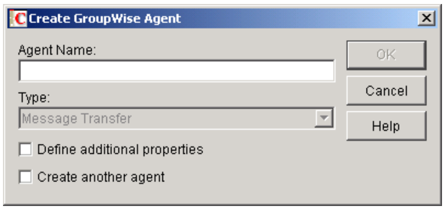
- “Creating an MTA Object in eDirectory” on page 575
- “Configuring the MTA in ConsoleOne” on page 577
- “Changing the Link Protocol between Domains” on page 579
- “Changing the Link Protocol between a Domain and Its Post Offices” on page 583
- “Moving the MTA to a Different Server” on page 586
- “Adjusting the MTA for a New Location of a Domain or Post Office” on page 587

Creating an MTA Object in eDirectory

When you create a new domain, an MTA object is automatically created for it. If the original MTA object for a domain gets accidently deleted, you can create a new one for it. Do not attempt to create more than one MTA object for a domain.

To create a new MTA object in Novell® eDirectory™:

1. In ConsoleOne®, browse to and right-click the Domain object for which you need to create an MTA object, then click New.
2. Double-click GroupWise Agent to display the Create GroupWise Agent dialog box.



Agent Name:

Type: Message Transfer

☐ Define additional properties

☐ Create another agent

3. Type a unique name for the new MTA. The name can include as many as 8 characters. Do not use any of the following invalid characters in the name:

   ASCII characters 0-13

   Asterisk *

   At sign @

   Braces { }

   Colon :

   Comma ,

   Double quote "

   Extended characters

   Parentheses ( )

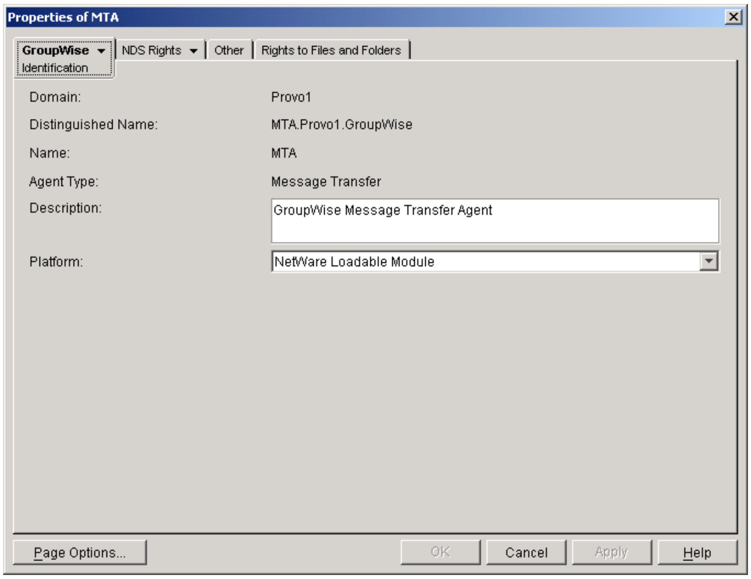
   Period .

   The Type field is automatically set to Message Transfer.

4. Select Define Additional Properties.
5. Click OK.

   The MTA object is automatically placed within the Domain object.

6. Review the information displayed for the first four fields on the Identification page to ensure that you are creating the correct type of Agent object in the correct location.



Domain: Provo1

Distinguished Name: MTA.Provo1.GroupWise

Name: MTA

Agent Type: Message Transfer

Description: GroupWise Message Transfer Agent

Platform: NetWare Loadable Module

7 In the Description field, type one or more lines of text describing the MTA. This description will display on the MTA agent console as the MTA runs.

If multiple administrators work at the server where the MTA will run, the description could include a note about who to contact before stopping the MTA. When running multiple MTAs on the same server, the description should uniquely identify each one. See Chapter 44, "Monitoring the MTA," on page 605.

8 In the Platform field, select the platform (NetWare Loadable Module or Windows) where the MTA will run.

9 Continue with "Configuring the MTA in ConsoleOne" on page 577.

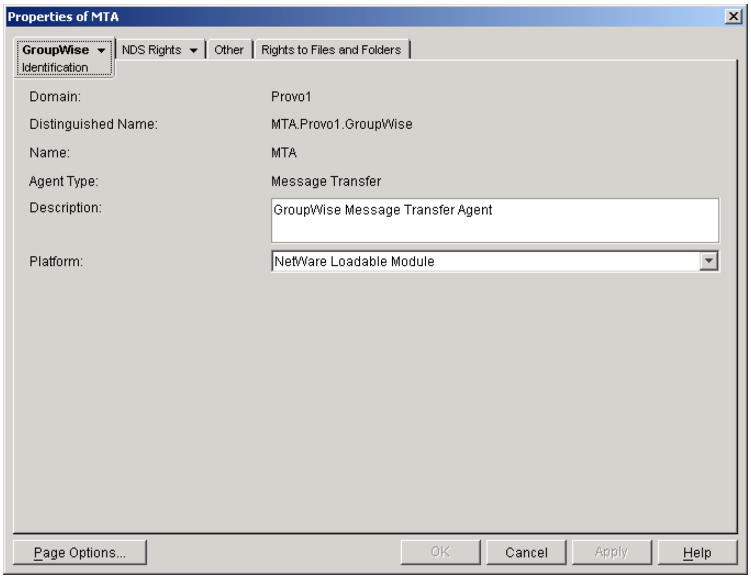
Configuring the MTA in ConsoleOne

The advantage to configuring the MTA in ConsoleOne, as opposed to using startup switches in an MTA startup file, is that the MTA configuration settings are stored in eDirectory.

1 In ConsoleOne, expand the eDirectory container where the Domain object is located.

2 Expand the Domain object.

3 Right-click the MTA object, then click Properties.



Domain: Provo1
Distinguished Name: MTA.Provo1.GroupWise
Name: MTA
Agent Type: Message Transfer
Description: GroupWise Message Transfer Agent
Platform: NetWare Loadable Module

The table below summarizes the MTA configuration settings in the MTA object properties pages and how they correspond to MTA startup switches (as described in Chapter 46, "Using MTA Startup Switches," on page 643):

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
Information Page	

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
Domain Distinguished Name Name Type Description Platform	See “Creating an MTA Object in eDirectory” on page 575.
Agent Settings Page	
Scan Cycle Scan High	See “Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways” on page 636. See also /cyhi and /cylo.
Attach Retry	See “Adjusting MTA Polling of Closed Locations” on page 640.
Enable Automatic Database Recovery	See /norecover.
Use 2nd High Priority Scanner Use 2nd Mail Priority Scanner	See “Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices” on page 638. See also /fast0 and /fast4.
SNMP Community "Get" String	See “Using SNMP Monitoring Programs” on page 627.
HTTP User Name HTTP Password	See “Setting Up the MTA Web Console” on page 617. See also /httpuser and /httppassword.
Network Address Page	
TCP/IP Address IPX/SPX Address	See “Using TCP/IP Links between Domains” on page 579 and “Using TCP/IP Links between a Domain and its Post Offices” on page 583. See also /tcpport.
Message Transfer	See “Using TCP/IP Links between Domains” on page 579. See also /msgtranssl.
HTTP	See “Setting Up the MTA Web Console” on page 617. See also /httpssl.
Log Settings Page	
Log File Path Logging Level Max Log File Age Max Log Disk Space	See “Using MTA Log Files” on page 625. See also /log, /logdays, /logdiskoff, /loglevel, and /logmax.
Message Log Settings Page	
Message Logging Level Message Log File Path	See “Enabling MTA Message Logging” on page 603. See also /messagelogsettings, /messagelogpath, /messagelogdays, and /messagelogmaxsize.
Scheduled Events Page	
eDirectory User Synchronization Event	See “Using eDirectory User Synchronization” on page 598. See also /nondssync.

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
Routing Options Page	
Default Routing Domain Force All Messages to Default Routing Domain	See "Using Routing Domains" on page 591. See also /defaultroutingdomain.
Allow MTA to Send Directly to Other GroupWise Systems	See "Using Dynamic Internet Links" in "Connecting to GroupWise 5.x and 6.x Systems" in the *GroupWise 6.5 Multi-System Administration Guide*. See also /nodns.
MTA SSL Page	
Certificate File SSL Key File Password	See "Enhancing Domain Security with SSL Connections to the MTA" on page 589. See also /certfile, /keyfile and /keypassword.

After you install the MTA software, you can further configure the MTA using a startup file. To survey the many ways the MTA can be configured, see Chapter 46, "Using MTA Startup Switches," on page 643.

Changing the Link Protocol between Domains

How MTAs for different domains communicate with each other is determined by the link protocol in use between the domains. Typically, inbound and outbound links for a domain use the same link protocol, but this is not required. For a review of link protocols, see "Link Protocols for Direct Links" on page 134.

If you originally set up an MTA using one link protocol and need to change to a different one, some reconfiguration of the MTA is necessary.

- "Using TCP/IP Links between Domains" on page 579
- "Using Mapped or UNC Links between Domains" on page 582
- "Using Gateway Links between Domains" on page 583

NOTE: The Linux MTA does not support mapped or UNC links between domains. TCP/IP links are required.

Using TCP/IP Links between Domains

To set up TCP/IP links between domains, you must perform the following two tasks:

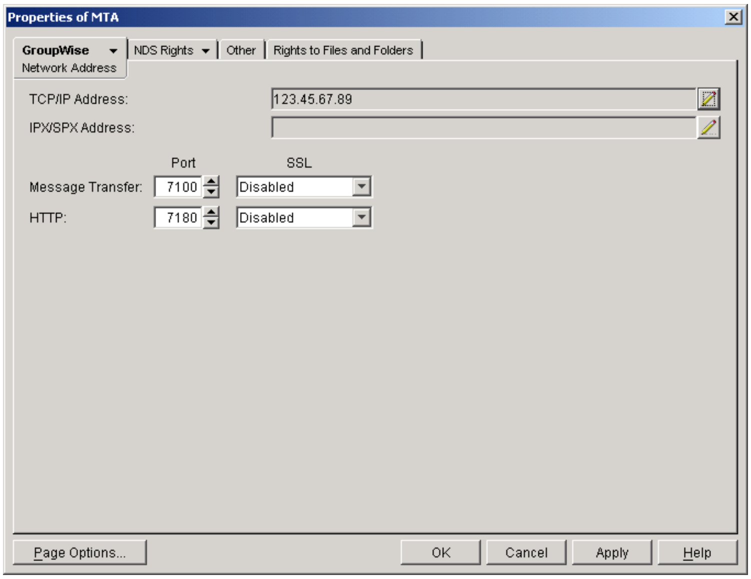
- "Configuring the MTA for TCP/IP" on page 579
- "Changing the Link Protocol between Domains to TCP/IP" on page 581

Configuring the MTA for TCP/IP

1 Make sure TCP/IP is properly set up on the server where the MTA is running.

2 In ConsoleOne, browse to and right-click the MTA object, then click Properties.

3 Click GroupWise > Network Address to display the Network Address page.

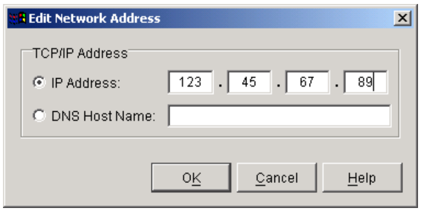


TCP/IP Address: 123.45.67.89

IPX/SPX Address:

	Port	SSL
Message Transfer:	7100	Disabled
HTTP:	7180	Disabled

4 On the Network Address page, click the pencil icon for the TCP/IP Address field to display the Edit Network Address dialog box.



● IP Address: 123 . 45 . 67 . 89

○ DNS Host Name:

5 Select IP Address, then provide the IP address, in dotted decimal format, of the server where the MTA is running.

or

Select DNS Host Name, then provide the DNS hostname of the server where the MTA is running.

IMPORTANT: The MTA must run on a server that has a static IP address. DHCP cannot be used to dynamically assign an IP address for it.

Specifying the DNS hostname rather than the IP address makes it easier to move the MTA from one server to another, should the need arise at a later time. You can assign a new IP address to the hostname in DNS, without needing to change the MTA configuration information in ConsoleOne.

6 Click OK.

7 To use a TCP port number other than the default port of 7100, type the port number in the Message Transfer Port field.

If multiple MTAs will run on the same server, each MTA must have a unique TCP port number.

8 If needed, select Enabled in the SSL drop-down list for the message transfer port. For more information, see "Enhancing Domain Security with SSL Connections to the MTA" on page 589.

9 Click OK to save the network address and return to the main ConsoleOne window.

ConsoleOne then notifies the MTA to restart enabled for TCP/IP.

Corresponding Startup Switches

You could also use the /tcpport switch in the MTA startup file to provide the message transfer port number.

MTA Web Console

You can view the MTA TCP/IP information on the Configuration page under the TCP/IP Settings heading.

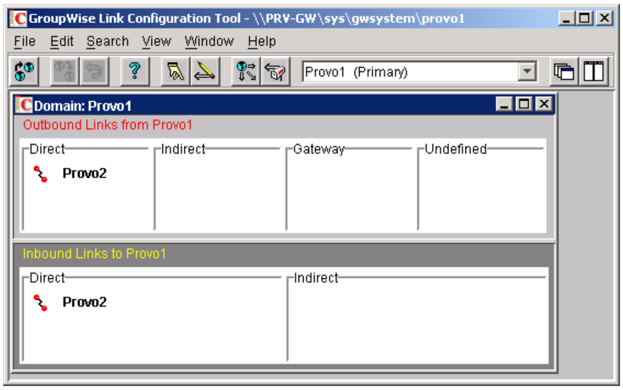
Changing the Link Protocol between Domains to TCP/IP

Make sure you have configured the MTA for TCP/IP at both ends of each link.

To change the link between the domains from mapped or UNC to TCP/IP:

1 In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.

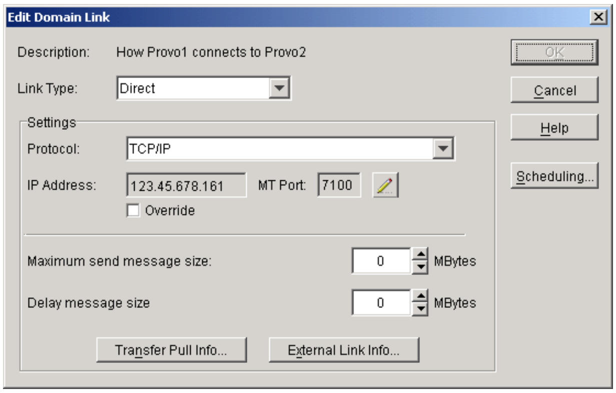
2 Click View > Domain Links to display domain links.


GroupWise Link Configuration Tool - \\PRV-GW\sys\gwsystem\provo1
File Edit Search View Window Help
Provo1 (Primary)
Domain: Provo1
Outbound Links from Provo1
Direct
Provo2
Indirect
Gateway
Undefined
Inbound Links to Provo1
Direct
Provo2
Indirect

3 Select the MTA's local domain in the drop-down list.

Outbound and inbound links for the selected domain are listed.

4 Double-click a domain in the Outbound Links list.


Edit Domain Link

Description: How Provo1 connects to Provo2

Link Type: Direct

Settings

Protocol: TCP/IP

IP Address: 123.45.678.161 MT Port: 7100

□ Override

Maximum send message size: 0 MBytes

Delay message size 0 MBytes

5 Set Link Type to Direct.

6 Set Protocol to TCP/IP.

Make sure the information displayed in the IP Address and MT Port fields matches the information for the MTA for the domain to which you are linking.

7 Click OK.

8. Repeat Step 4 through Step 7 for each domain in the Outbound Links list where you want the MTA to use a TCP/IP link.

   Selecting multiple domains is also allowed.

9. Double-click a domain in the Inbound Links list.
10. Set Link Type to Direct.
11. Set Protocol to TCP/IP.

    Make sure the information displayed in the IP Address and MT Port fields matches the information you supplied in "Configuring the MTA for TCP/IP" on page 579.

12. Click OK.
13. Repeat Step 9 through Step 12 for each domain in the Inbound Links list where you want the MTA to use a TCP/IP link.

    Selecting multiple domains is also allowed.

14. Click File > Exit > Yes to save the link changes.

    ConsoleOne then notifies the MTA to restart with the new link configuration.

For a sample message flow for this configuration, see "TCP/IP Link Open: Transfer between Domains Successful" in "Message Delivery to a Different Domain" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Using Mapped or UNC Links between Domains

To change to a mapped or UNC link between domains:

1. In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.
2. Click View > Domain Links to display domain links.
3. Select the MTA's local domain in the drop-down list.

   Outbound and inbound links for the selected domain are listed.

4. Double-click a domain in the Outbound Links list.
5. Set Link Type to Direct.
6. Set Protocol to Mapped or UNC.
7. Enter the full path, in the appropriate format, of the directory where the other domain is located.
8. Click OK.
9. Repeat Step 4 through Step 8 for each domain in the Outbound Links list where you want the MTA to use a mapped or UNC link.

   Selecting multiple domains is also allowed.

10. Double-click a domain in the Inbound Links list.
11. Set Link Type to Direct.
12. Set Protocol to Mapped or UNC.
13. Enter the full path, in the appropriate format, of the directory where the local domain is located.
14. Click OK.

15 Repeat Step 10 through Step 14 for each domain in the Inbound Links list where you want the MTA to use a mapped link.

Selecting multiple domains is also allowed.

16 Click File > Exit > Yes to save the link changes.

ConsoleOne then notifies the MTA to restart with the new link configuration.

For a sample message flow for this configuration, see "Mapped/UNC Link Open: Transfer between Domains Successful" in "Message Delivery to a Different Domain" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Using Gateway Links between Domains

You can use GroupWise gateways to link domains within your GroupWise system.

- "Using the Async Gateway to Link Domains" on page 583
- "Using the Internet Agent to Link Domains" on page 583

Using the Async Gateway to Link Domains

You can use the Async Gateway to link a domain into your GroupWise system using a modem. For setup instructions, see the Async Gateway documentation at GroupWise 6.5 Documentation (http://www.novell.com/documentation/gw65/index.html).

Using the Internet Agent to Link Domains

You can use the Internet Agent to link a domain into your GroupWise system across the Internet. When you use the Internet Agent as the transport mechanism between domains, it encapsulates GroupWise messages (both e-mail messages and administrative messages) within SMTP messages in order to transport them across the Internet. For setup instructions, see "Linking Domains" on page 762

NOTE: A simpler alternative to a gateway link for spanning the Internet is to use MTA to MTA links, as described for linking separate GroupWise systems in "Using Dynamic Internet Links" in the *GroupWise 6.5 Multi-System Administration Guide*. The same configuration that can link two separate GroupWise systems can be employed to link a domain within the same GroupWise system.

Changing the Link Protocol between a Domain and Its Post Offices

How messages are transferred between the MTA for the domain and the POA for each post office is determined by the link protocol in use between the domain and each post office. For a review of link protocols, see "Link Protocols for Direct Links" on page 134.

If you need to change from one link protocol to another, some reconfiguration of the MTA and its link to each post office is necessary.

- "Using TCP/IP Links between a Domain and its Post Offices" on page 583
- "Using Mapped or UNC Links between a Domain and its Post Offices" on page 586

NOTE: The Linux MTA requires TCP/IP links between a domain and its post offices.

Using TCP/IP Links between a Domain and its Post Offices

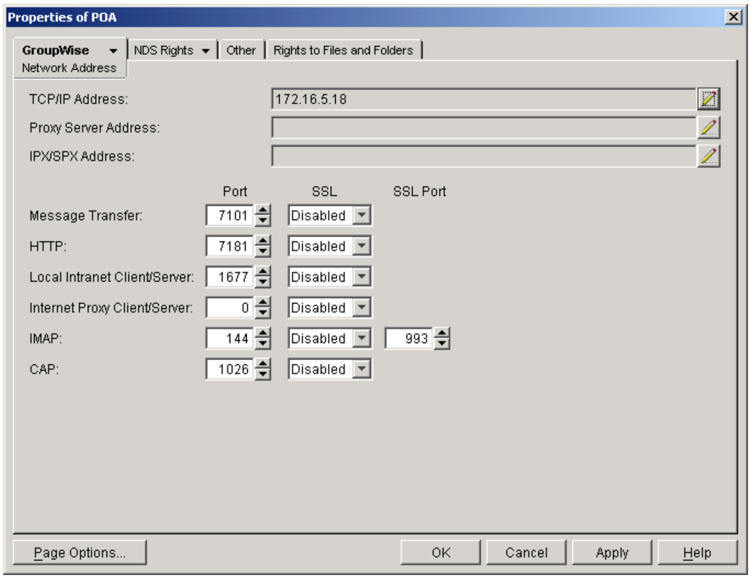
To change from mapped or UNC links to TCP/IP links between a domain and its post offices, you must perform the following two tasks:

- "Configuring the Agents for TCP/IP" on page 584
- "Changing the Link Protocol between a Domain and its Post Offices to TCP/IP" on page 585

Configuring the Agents for TCP/IP

1. If the MTA for the domain is not yet set up for TCP/IP communication, see "Configuring the MTA for TCP/IP" on page 579.
2. If any post offices do not yet have a POA set up for TCP/IP communication, see "Using Client/Server Access to the Post Office" on page 447 to set up the initial TCP/IP information.
3. In ConsoleOne, expand the Post Office object to display the POA object(s) in the post office.

   Only one POA per post office needs to communicate with the MTA. If the post office has multiple POAs, have a POA that performs message file processing communicate with the MTA for best performance. For information about message file processing, see "Role of the Post Office Agent" on page 423.
4. Right-click the POA object, then click Properties.
5. Click GroupWise > Network Address to display the Network Address page.



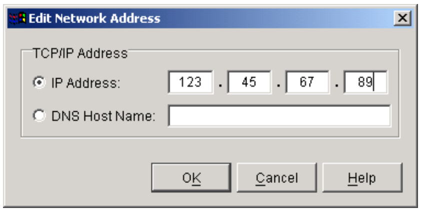
TCP/IP Address: 172.16.5.18

Proxy Server Address:

IPX/SPX Address:

	Port	SSL	SSL Port
Message Transfer:	7101	Disabled	
HTTP:	7181	Disabled	
Local Intranet Client/Server:	1677	Disabled	
Internet Proxy Client/Server:	0	Disabled	
IMAP:	144	Disabled	993
CAP:	1026	Disabled	

6. On the Network Address page, click the pencil icon for the TCP/IP Address field to display the Edit Network Address dialog box.



● IP Address: 123 . 45 . 67 . 89

○ DNS Host Name:

7. In the Message Transfer Port field, specify a unique TCP port on which the POA will listen for incoming messages from the MTA.

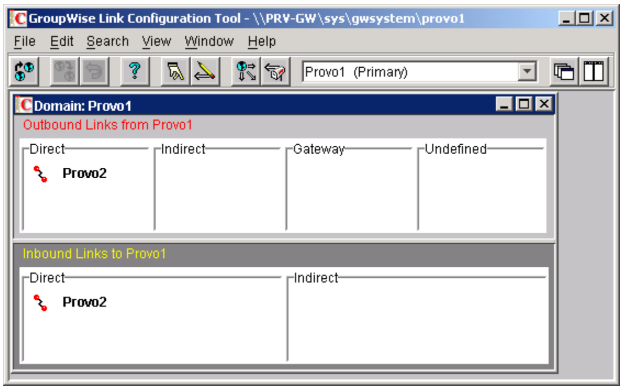
   The default is 7101.
8. If needed, select Enabled in the SSL drop-down list for the message transfer port. For more information, see "Enhancing Domain Security with SSL Connections to the MTA" on page 589.

9. Click OK to save the TCP/IP information and return to the main ConsoleOne window.

   ConsoleOne then notifies the POA to restart with message transfer processing enabled.

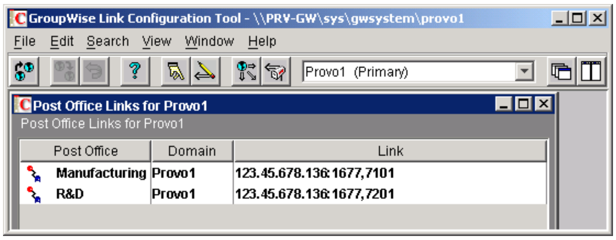
Changing the Link Protocol between a Domain and its Post Offices to TCP/IP

1. In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.


GroupWise Link Configuration Tool - \\PRV-GW\sys\gwsystem\provo1
File Edit Search View Window Help
Provo1 (Primary)
Domain: Provo1
Outbound Links from Provo1
Direct
Provo2
Indirect
Gateway
Undefined
Inbound Links to Provo1
Direct
Provo2
Indirect

2. In the drop-down list, select the domain where you want TCP/IP links to post offices.

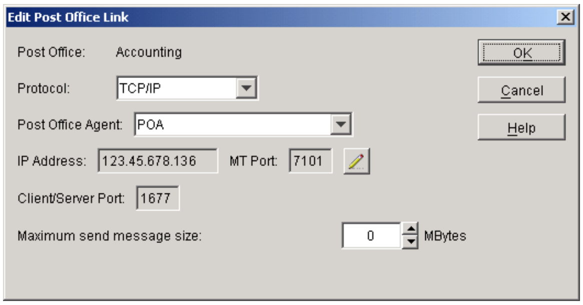
3. Click View > Post Office Links to display post office links.


GroupWise Link Configuration Tool - \\PRV-GW\sys\gwsystem\provo1
File Edit Search View Window Help
Provo1 (Primary)
Post Office Links for Provo1
Post Office Links for Provo1

Post Office	Domain	Link
Manufacturing	Provo1	123.45.678.136:1677,7101
R&D	Provo1	123.45.678.136:1677,7201

4. Double-click a Post Office object.

5. In the Protocol field, select TCP/IP.



Post Office: Accounting

Protocol: TCP/IP

Post Office Agent: POA

IP Address: 123.45.678.136 MT Port: 7101

Client/Server Port: 1677

Maximum send message size: 0 MBytes

6. Make sure the information displayed in the Edit Post Office Link dialog box matches the information provided in the Edit Network Address dialog box in "Configuring the Agents for TCP/IP" on page 584.

7. Click OK.

8. Repeat Step 4 through Step 7 for each post office in the domain where you want to use TCP/IP links.

9 To exit the Link Configuration tool and save your changes, click File > Exit > Yes.

ConsoleOne then notifies the MTA and POAs to restart using the new link protocol.

For a sample message flow for this configuration, see "TCP/IP Link Open: Transfer between Post Offices Successful" in "Message Delivery to a Different Post Office" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Using Mapped or UNC Links between a Domain and its Post Offices

To change from a TCP/IP link to a mapped or UNC link between a domain and its post offices:

1 In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.

2 In the drop-down list, select the domain where the post offices reside.

3 Click View Post Office Links to display post office links.

4 Double-click a Post Office object.

5 In the Protocol field, select Mapped or UNC.

6 Provide the location of the post office in the format appropriate to the selected protocol.

7 Click OK.

8 Repeat Step 4 through Step 7 for each post office in the domain.

9 To exit the Link Configuration tool and save your changes, click File > Exit > Yes.

ConsoleOne then notifies the POA and MTA to restart using the new link protocol.

For a sample message flow for this configuration, see "Mapped/UNC Link Open: Transfer between Post Offices Successful" in "Message Delivery to a Different Post Office" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

Moving the MTA to a Different Server

As your GroupWise system grows and evolves, you might need to move an MTA from one server to another. For example, you might decide to run the MTA on a different platform, or perhaps you want to move it to a server that has more disk space for the mslocal directory.

1 Stop the existing MTA.

2 Copy the entire mslocal subdirectory structure to wherever you want it on the new server. It might contain messages that have not yet been delivered.

3 When moving the MTA, pay special attention to the following details:

- In the MTA startup file, set the /work switch to the location of the mslocal directory on the new server.
- If the original MTA was configured for TCP/IP links between domains, you must reconfigure the MTA object with the IP address and port number for the MTA on the new server. See "Using TCP/IP Links between Domains" on page 579.
- For the NetWare® MTA, if it was originally on the same server where its domain and post offices are located and you are moving it to a different server, you must add the /dn switch or the /user and /password switches to the MTA startup file to give the NetWare MTA access to the server where the domain and post offices are located.

4 Install the MTA on the new server. See "Installing GroupWise Agents" in the *GroupWise 6.5 Installation Guide*.

5. Start the new MTA. See "Starting the MTA" on page 568.
6. Observe the new MTA to see that it is running smoothly. See Chapter 44, "Monitoring the MTA," on page 605.
7. If you are no longer using the old server for any GroupWise agents, you can remove them to reclaim the disk space. See "Uninstalling the MTA Software" on page 573.

Adjusting the MTA for a New Location of a Domain or Post Office

MTA configuration must be adjusted if you make the following changes to your GroupWise system configuration:

- "New Domain Location" on page 587
- "New Post Office Location" on page 587

New Domain Location

If you move a domain from one server to another, you need to edit the MTA startup file to provide the new location of the domain directory.

1. Stop the MTA for the old domain location if it is still running.
2. Use an ASCII text editor to edit the MTA startup file.
    - On NetWare and Windows, only the first 8 characters of the domain name are used in the filename. The startup file is typically located in the directory where the MTA software is installed.
    - On Linux, the full domain name is used in the filename. However, all letters are lowercase and any spaces in the domain name are removed. The startup file is located in the /opt/novell/groupwise/agents/share directory.
3. Adjust the setting of the /home switch to point to the new location of the domain directory.
4. Save the MTA startup file.
5. Start the MTA for the new domain location. See "Starting the MTA" on page 568.

New Post Office Location

If you move a post office, you need to adjust the link information for that post office.

1. Click Tools > GroupWise Utilities > Link Configuration.
2. In the drop-down list, select the domain where a post office has moved.
3. Click View > Post Office Links to display post office links.
4. Double-click the post office that has been moved.
5. Provide its new location in the appropriate format.
6. Click OK.
7. Click File > Exit > Yes to save the link changes.

   ConsoleOne then notifies the MTA to restart with the new link configuration.

Adjusting the MTA Logging Level and Other Log Settings

When installing or troubleshooting the MTA, a logging level of Verbose can be useful. However, when the MTA is running smoothly, you can set the logging level down to Normal to conserve disk space occupied by log files. See "Using MTA Log Files" on page 625.

Configuring User Access through the Domain

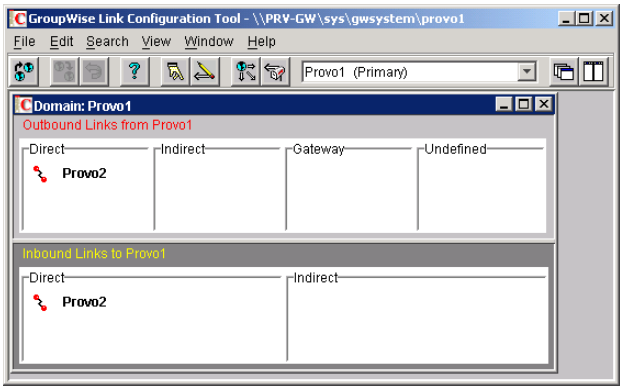
Although users do not access the domain as they use the GroupWise client, their messages often pass through domains while traveling from one post office to another.

- "Restricting Message Size between Domains" on page 588
- "Enabling Live Remote" on page 589
- "Enhancing Domain Security with SSL Connections to the MTA" on page 589

Restricting Message Size between Domains

You can configure the MTA to restrict the size of messages that users are permitted to send outside the domain.

1 In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.



GroupWise Link Configuration Tool - \\PRV-GW\sys\gwsystem\provo1

Provo1 (Primary)

Domain: Provo1

Outbound Links from Provo1

Direct: Provo2

Indirect

Gateway

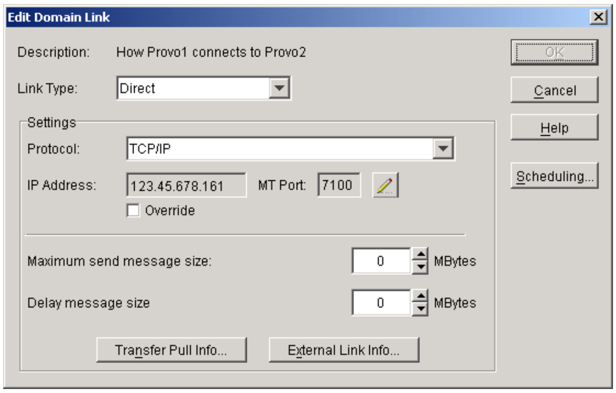
Undefined

Inbound Links to Provo1

Direct: Provo2

Indirect

2 Double-click the domain where you want to restrict message size.



Edit Domain Link

Description: How Provo1 connects to Provo2

Link Type: Direct

Settings

Protocol: TCP/IP

IP Address: 123.45.678.161

MT Port: 7100

☐ Override

Maximum send message size: 0 MBytes

Delay message size 0 MBytes

3 In the Maximum Send Message Size field, specify in megabytes the size of the largest message you want users to be able to send outside the post office.

4. If you want to delay large messages, specify the size in megabytes for message files the MTA can process immediately in the Delay Message Size field.

   If a message file exceeds the delay message size, the message file is moved into the low priority (6) message queue, where only one MTA thread is allocated to process very large messages. This arrangement allows typical messages to be processed promptly, while delaying large messages that exceed the specified size. The result is that large messages do not slow down processing of typical messages.

5. Click OK.

6. To exit the Link Configuration Tool and save your changes, click File > Exit > Yes.

ConsoleOne then notifies the MTA to restart using the new message size limits.

If a user's message is not sent out of the domain because of this restriction, the user receives an e-mail message with a subject line of:

```
Delivery disallowed
```

plus the subject of the original message. This message provides information to the user about why and where the message was disallowed. However, the message is still delivered to recipients in the sender's own domain.

There are additional ways to restrict the size of messages that users can send, as described in "Restricting the Size of Messages That Users Can Send" on page 175.

Enabling Live Remote

You can configure the MTA to redirect GroupWise Remote client requests to other MTAs and POAs. The GroupWise client can establish a client/server connection to an MTA across the Internet, eliminating the queuing and polling process used by earlier Remote clients. The result is significantly improved performance for Remote client users.

To configure the MTA to redirect Remote client requests, add the /liveremote, /lrconn and /lrwaitdata switches to the MTA startup file.

You can monitor the live remote connections from the MTA agent console. See "Displaying Live Remote Status" on page 613.

As an alternative to live remote connections from outside your firewall, you could set up proxy servers for the POAs, so that Remote client users connect to their mailboxes through the proxy servers rather than through MTAs. Full SSL security is provided through the proxy servers. See "Securing Client/Server Access through a Proxy Server" on page 456.

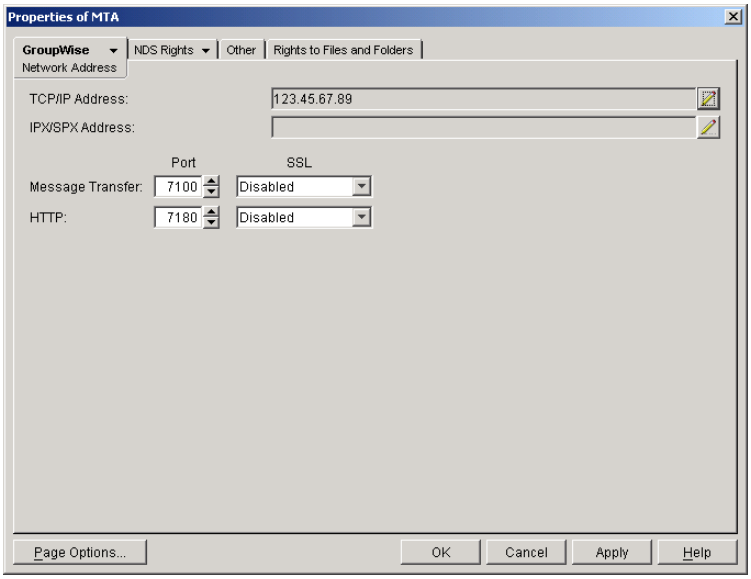
Enhancing Domain Security with SSL Connections to the MTA

Secure Sockets Layer (SSL) ensures secure communication between the MTA and other programs by encrypting the complete communication flow between the programs. For background information about SSL and how to set it up on your system, see Chapter 80, "Encryption and Certificates," on page 1039.

To configure the MTA to use SSL:

1. In ConsoleOne, browse to and right-click the MTA object, then click Properties.

2. Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 123.45.67.89

IPX/SPX Address:

	Port	SSL
Message Transfer:	7100	Disabled
HTTP:	7180	Disabled

3 To use SSL connections between the MTA and the POAs for its post offices, select Enabled in the Message Transfer SSL drop-down list.

The MTA must use a TCP/IP connection to each POA in order to enable SSL for the connection. See "Using TCP/IP Links between a Domain and its Post Offices" on page 583.

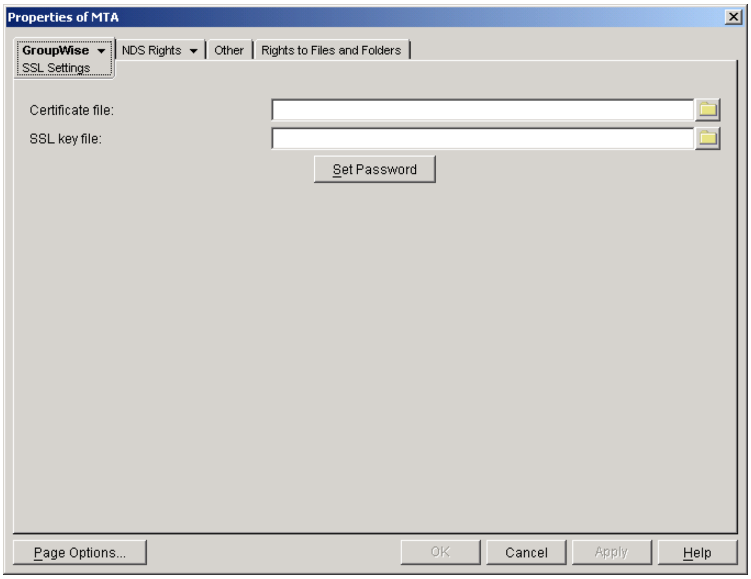
Each POA must also have SSL enabled for the connection to be secure. See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.

4 To use SSL connections between the MTA and the MTA Web console displayed in your Web browser, select Enabled in the HTTP SSL drop-down list.

To set up the MTA Web console, see "Setting Up the MTA Web Console" on page 617.

5 Click Apply to save the settings on the Network Address page.

6 Click GroupWise > SSL Settings to display the SSL Settings page.



Certificate file:

SSL key file:

For background information about certificate files and SSL key files, see Chapter 80, "Encryption and Certificates," on page 1039.

7 In the Certificate File field, browse to and select the public certificate file provided to you by your CA.

8 In the SSL Key File field:

8a Browse to and select your private key file.

8b Click Set Password.

8c Provide the password that was used to encrypt the private key file when it was created.

8d Click Set Password.

9 Click OK to save the SSL settings.

ConsoleOne then notifies the MTA to restart using the new message size limits.

Corresponding Startup Switches
You could also use the /certfile, /keyfile, /keypassword, /httpssl, and /msgtranssl switches in the MTA startup file to configure the MTA to use SSL.

MTA Web Console
You can list which connections the MTA is using SSL for from the Links page. Click View TCP/IP Connections to display the list if TCP/IP links.

Configuring Specialized Routing

As you create each new domain in your GroupWise system, you link it to another domain. You can view and modify the links between domains using the Link Configuration Tool. See Chapter 10, "Managing the Links between Domains and Post Offices," on page 131. The following topics help you configure the MTA to customize routing through your GroupWise system:

- "Using Routing Domains" on page 591
- "Scheduling Direct Domain Links" on page 593
- "Using a Transfer Pull Configuration" on page 596

Using Routing Domains

As an alternative to configuring individual links between individual domains throughout your GroupWise system, you can establish a system of one or more routing domains under the following circumstances.

- Domains must connect to the routing domains with TCP/IP links.
- GroupWise 5.5 and 6.*x* domains can be part of the routing domain system. Domains and MTAs that are still at a 5.2 or earlier version cannot participate and must use links as provided in the Link Configuration Tool.

A routing domain can serve as a hub in the following situations:

- Messages that would otherwise be undeliverable can be automatically sent to a single routing domain. This routing domain could be set up to perform DNS lookups and route messages out across the Internet. See "Using Dynamic Internet Links" in "Connecting to GroupWise 5.x and 6.x Systems" in the *GroupWise 6.5 Multi-System Administration Guide*.

- All messages from a domain can be automatically routed through another domain, regardless of the final destination of the messages. This provides additional control of message flow through your GroupWise system.

You can set up routing domains on two levels:

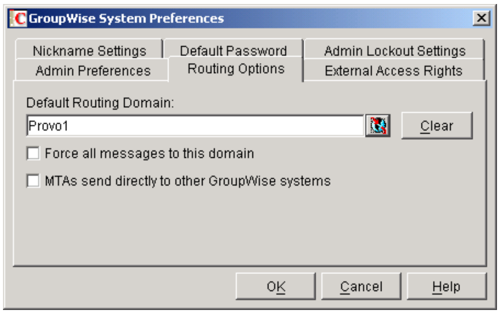
- "Selecting a System Default Routing Domain" on page 592
- "Selecting a Specific Routing Domain for an Individual Domain" on page 593

Selecting a System Default Routing Domain

You can establish a single default routing domain for your entire GroupWise system. This provides a centralized routing point for all messages. It takes precedence over specific links established when domains were created or links modified with the Link Configuration Tool.

To set up a system default routing domain:

1. In ConsoleOne, click Tools > GroupWise System Operations > System Preferences > Routing to display the Routing tab.



Default Routing Domain: Provo1

□ Force all messages to this domain

□ MTAs send directly to other GroupWise systems

2. In the Default Routing Domain field, browse to and select the domain you want to serve as the default routing domain for your entire GroupWise system.
3. If you want all GroupWise messages to pass through the default routing domain regardless of the destination of the message, select Force All Messages to This Domain.

   or

   If you want only undeliverable GroupWise messages to be routed to the default routing domain, deselect Force All Messages to This Domain.

   If you do not force all messages to the system default routing domain, then you have the option of allowing selected MTAs to provide routing domain services in addition to the system default routing domain.
4. Select MTAs Send Directly to Other GroupWise Systems if you want all MTAs in your GroupWise system to perform DNS lookups and route messages out across the Internet.

   or

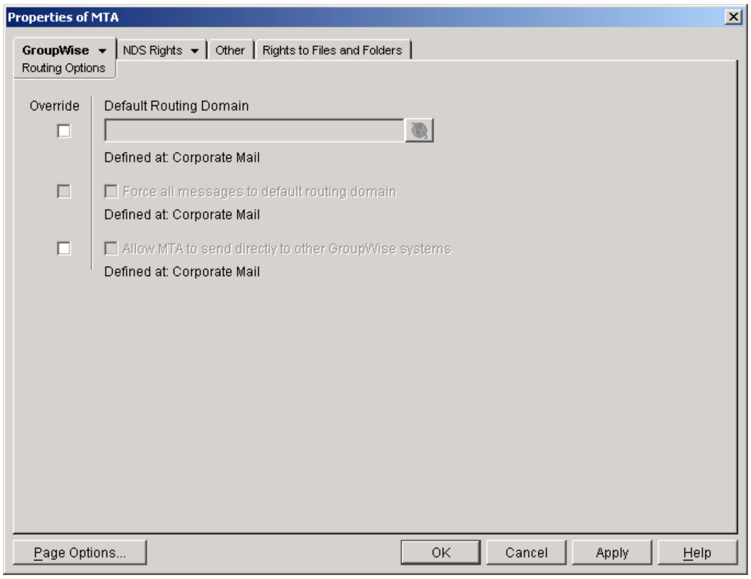
   Deselect MTAs Send Directly to Other GroupWise systems if you want to individually designate which MTAs should perform eDirectory lookups and route messages out across the Internet.
5. Click OK to save the routing options you have specified for the system default routing domain.

Selecting a Specific Routing Domain for an Individual Domain

As long as you are not forcing all messages to the system default routing domain, you can override the system default routing information for an individual domain.

1 In ConsoleOne, browse to and right-click the MTA object, then click Properties.

2 Click GroupWise > Routing Options to display the Routing Options page.



Override | Default Routing Domain

□

Defined at: Corporate Mail

□ □ Force all messages to default routing domain

Defined at: Corporate Mail

□ □ Allow MTA to send directly to other GroupWise systems

Defined at: Corporate Mail

System default routing information displays if it has been set up. See “Selecting a System Default Routing Domain” on page 592.

3 Select Override beside the default information you want to change for the selected domain.

4 Set the routing options as needed for the selected domain.

5 Click OK to save the specialized routing information for the selected domain.

ConsoleOne then notifies the MTA to restart so the routing information can be put into effect.

MTA Web Console

You can check routing information on the Configuration page under the General Settings heading.

Scheduling Direct Domain Links

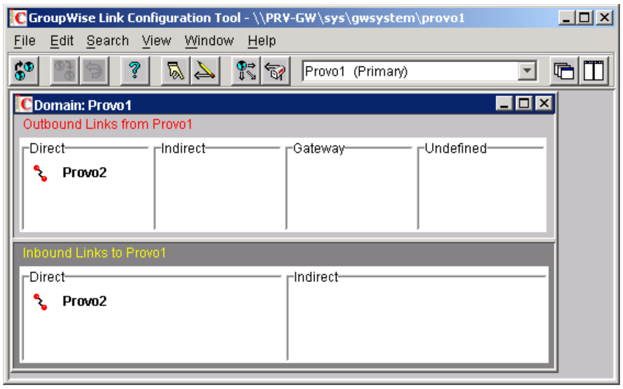
When domains link across an expensive medium such as long-distance phone lines, you can reduce the cost of the link by controlling when it is open. You can choose to have some types of messages wait in the message queues for the lowest phone rate. You can collect messages in the message queues until a specified time or size limit is reached, then open the link, rather than opening the link for each message as it arrives in the queue. You can design as many link profiles as you need, to schedule the transfer of various types of GroupWise messages in the most efficient and cost-effective manner.

To create a schedule for a link between domains:

1 In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.

2 In the drop-down list, select the domain to schedule a link for.

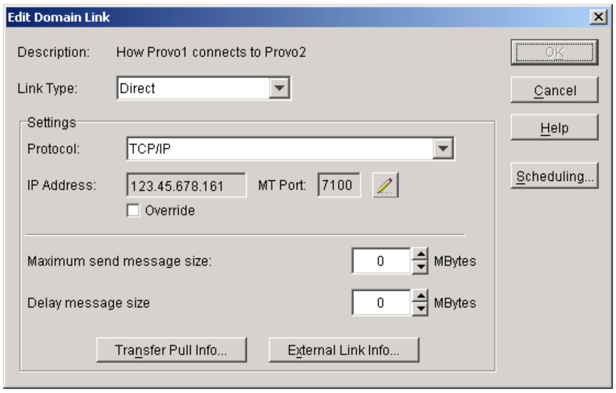
3 Click View > Domain Links to display domain links.


GroupWise Link Configuration Tool - \\PRV-GW\sys\gwsystem\provo1
File Edit Search View Window Help
Domain: Provo1
Outbound Links from Provo1
Direct
Provo2
Indirect
Gateway
Undefined
Inbound Links to Provo1
Direct
Provo2
Indirect

Provo1 (Primary)

4 Double-click the domain you want to create a link schedule for.

Only direct links can be scheduled.



Description: How Provo1 connects to Provo2

Link Type: Direct

Protocol: TCP/IP

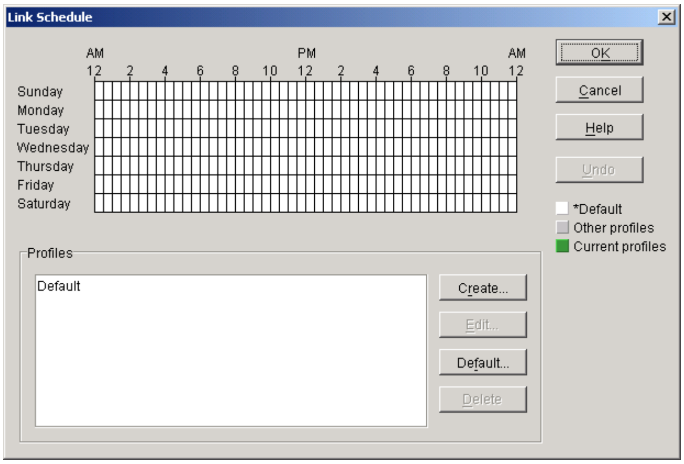
IP Address: 123.45.678.161 MT Port: 7100

□ Override

Maximum send message size: 0 MBytes

Delay message size 0 MBytes

5 Click Scheduling.



□ *Default

□ Other profiles

🟩 Current profiles

Profiles

Default

The link schedule grid displays the current schedule for the selected direct link. The grid consists of half-hour time slots showing the link profile assigned to each time slot. Available link profiles are listed below the link schedule grid.

Each link profile defines the following values to set the conditions under which the link opens:

- Which message queues to monitor
- Maximum wait time for any message in any monitored queue

- Maximum number of waiting messages allowed in all monitored queues
- Maximum total size of waiting messages allowed in all monitored queues

The default profile shows as white in the link schedule grid. The default profile is in effect at all times when no other profile has been selected. Any other defined profiles show as gray. The currently selected link profile shows as green.

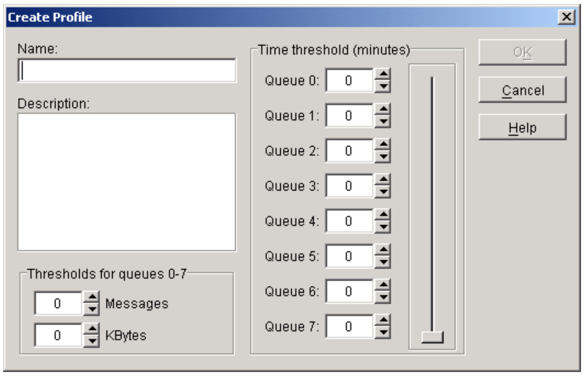
6 To create a new link profile, click Create.

or

To edit an existing link profile, select it in the profile list, then click Edit.

or

To edit the default link profile, click Default.



Name:

Description:

Thresholds for queues 0-7

0 Messages

0 KBytes

Time threshold (minutes)

Queue 0: 0

Queue 1: 0

Queue 2: 0

Queue 3: 0

Queue 4: 0

Queue 5: 0

Queue 6: 0

Queue 7: 0

7 If you are creating a new link profile, provide a unique name for the link profile in the Name field.

If you are editing an existing link profile, you cannot change the name.

8 In the Description field, provide whatever additional information is necessary to describe the purpose of the link profile.

9 Use the scroll bar in the Time Threshold box to select which queues to monitor and process when this link profile is in effect.

Queue	Purpose
0	Busy Search requests
1	Requests from GroupWise Remote users
2	High priority user messages; administrative messages
3	High priority status messages
4	Normal priority user messages
5	Normal priority status messages
6	Low priority user messages
7	Low priority status messages

The contents of deselected queues are not monitored but are processed when the link opens.

10 For each selected queue, specify the maximum number of minutes a message must wait in each queue before the link opens.

If you want the link to open immediately when a message arrives in the queue, specify 0 (zero).

11 In the Messages field, specify the total number of messages waiting in all selected queues that will trigger the link to open.

12 In the KBytes field, specify the total size in kilobytes of all messages waiting in all selected queues that will trigger the link to open.

13 Click OK to save the link profile and return to the Link Scheduling dialog box.

14 Select the new or modified link profile in the profile list.

15 Click a time slot or drag to select a range of time slots.

Time slots assigned to the selected link profile display as green.

16 Select all the time slots you want governed by the selected link profile.

17 Select a different link profile to assign to time slots.

or

Create or edit another link profile.

or

Click OK to save the schedule for the current link.

18 When the schedule is saved, click OK to close the Edit Domain Link dialog box.

19 To exit the Link Configuration Tool, click File > Exit > Yes.

ConsoleOne then notifies the MTA to restart using the new link schedule.

Using a Transfer Pull Configuration

Typically for a mapped or UNC link, the MTA for the sending domain writes (or "pushes") message files into the input queue subdirectories of the receiving domain. However, it is possible to change this configuration so the MTA for the receiving domain picks up (or "pulls") message files from the sending domain.

The transfer pull directory is a location in the sending domain where the MTA for the receiving domain can pick up message files (that is, "pull" them from the sending domain). It represents the only configuration where an MTA processes messages outside its own domain directory structure.

NOTE: The transfer pull configuration does not apply to the Linux MTA because the Linux MTA does not use mapped or UNC links.

To set up a transfer pull configuration between domains:

1 Manually create a transfer directory with input queue subdirectories from which outgoing message files will be pulled.

The transfer directory must contain a wpcsin subdirectory, with standard priority 0 through 7 subdirectories beneath. For an example, see “Alternate Link Configuration: Transfer Pull” in “Message Delivery to a Different Domain” in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*. The transfer directory must be placed where both the sending and receiving MTAs have rights.

2 In ConsoleOne, modify the outgoing link from the sending domain so the MTA for the sending domain writes message files to the transfer directory, rather than directly to the receiving domain. See "Modifying the Outgoing Transfer Pull Link" on page 597.

3 In ConsoleOne, modify the incoming link to the receiving domain so the MTA for the receiving domain actively pulls message files from the transfer directory, rather than waiting for them to be delivered. See "Modifying the Incoming Transfer Pull Link" on page 597.

4 Stop and restart the MTAs for both domains.

Modifying the Outgoing Transfer Pull Link

1 In ConsoleOne, connect to the sending domain:

1a Click Tools > GroupWise System Operations > Select Domain.

1b Browse to and select the domain database (wpdomain.db) in the sending domain.

1c Click Open.

1d Click OK.

2 Click Tools > GroupWise Utilities > Link Configuration.

3 In the drop-down list, select the sending domain.

4 Click View > Domain Links to view outbound and inbound links for the sending domain.

5 In the Outbound Links from *sending_domain_name* list box, double-click the receiving domain.

6 If you are using a UNC path, click Override to display the Path field.

7 In the Path or UNC Override field (depending on the selected protocol), specify the full path to the transfer directory you created.

You can use a UNC path for the NetWare and Windows MTA; you can use a mapped drive path for the Windows MTA only.

8 Click OK.

9 Click File > Exit > Yes to save the link changes for the sending domain and return to the main ConsoleOne window.

10 Continue with "Modifying the Incoming Transfer Pull Link" on page 597.

Modifying the Incoming Transfer Pull Link

1 In ConsoleOne, connect to the receiving domain:

1a Click Tools > GroupWise System Operations > Select Domain

1b Browse to and select the domain database (wpdomain.db) in the receiving domain.

1c Click Open.

1d Click OK.

2 Click Tools > GroupWise Utilities > Link Configuration.

3 In the drop-down list, select the receiving domain.

4 Click View Domain Links to view outbound and inbound links for the receiving domain.

5 In the Outbound Links from *receiving_domain_name* list box, double-click the sending domain.

6. Verify that the information displayed in the Edit Domain Link dialog box is correct.
7. Click Transfer Pull Info.
8. Specify the full path to the transfer directory you created.

   You can use a UNC path for the NetWare and Windows MTA; you can use a mapped drive path for the Windows MTA only.
9. Specify the number of seconds after which the MTA will check the transfer directory for message files to pull.
10. Specify the command needed to reestablish the connection with the transfer directory, if that connection should be broken for any reason.
11. Click OK until you return to the Link Configuration dialog box.
12. Click File > Exit > Yes to save the link changes for the receiving domain and return to the main ConsoleOne window.
13. Stop and restart the MTAs for both domains.

Configuring Domain Maintenance

You can configure the MTA to synchronize user information in the GroupWise Address Book with user information in eDirectory. You can also configure it to gather information about all messages that pass through the domain for tracking purposes.

- "Using eDirectory User Synchronization" on page 598
- "Enabling MTA Message Logging" on page 603

Using eDirectory User Synchronization

As long as GroupWise administration is performed with the GroupWise Administrator snap-in to ConsoleOne running, user information is automatically synchronized between GroupWise and eDirectory. However, four situations can cause this automatic synchronization to be insufficient:

- An administrator modifies user information in ConsoleOne without having the GroupWise Administrator snap-in running.
- The user information was changed using NetWare® Administrator without the GroupWise Administrator snap-in running.
- The user information was changed using NetAdmin, the DOS-based NetWare Administrator program.
- The user information was changed using the NWDS API.

In these situations, user information in eDirectory would no longer match corresponding user information in GroupWise. (User objects are the only GroupWise objects that can be modified without the GroupWise Administrator snap-in running. Modification of all other GroupWise objects requires the presence of the GroupWise Administrator snap-in.)

This section covers the following aspects of eDirectory user synchronization:

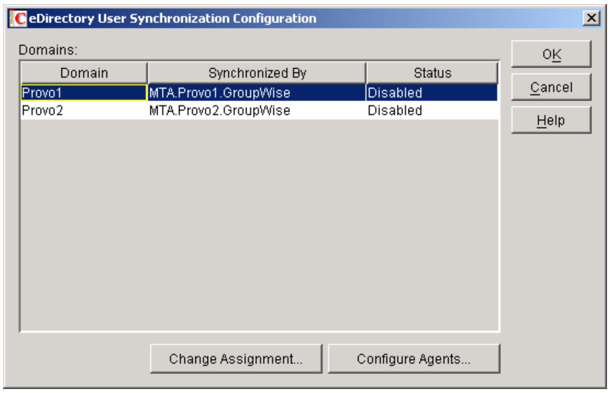
- "Enabling eDirectory User Synchronization" on page 599
- "Assigning an eDirectory-Enabled MTA to Synchronize Other Domains" on page 601
- "Scheduling eDirectory User Synchronization" on page 602

Enabling eDirectory User Synchronization

By default, eDirectory user synchronization is disabled. The MTA still performs all its other functions, but any changes made to user information in eDirectory without the GroupWise Administrator snap-in running will not appear in GroupWise until eDirectory user synchronization has been performed.

Although all MTAs could be enabled to perform eDirectory user synchronization, the minimum requirement is that at least one MTA be configured that way. If your GroupWise system spans multiple trees, at least one MTA in each tree must be configured to perform eDirectory user synchronization.

1 In ConsoleOne, click Tools > GroupWise System Operations > eDirectory User Synchronization to display the eDirectory User Synchronization Configuration dialog box.



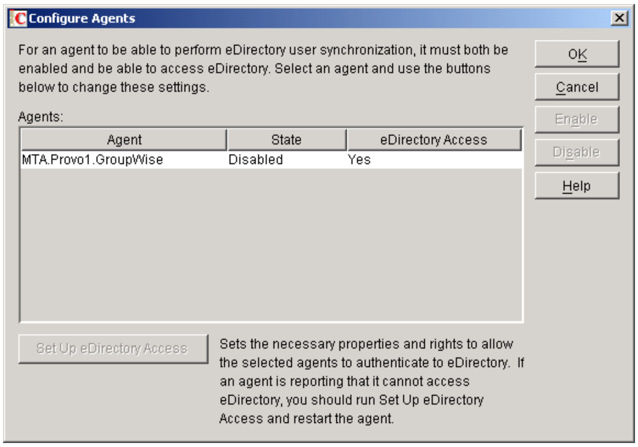
eDirectory User Synchronization Configuration

Domains:

Domain	Synchronized By	Status
Provo1	MTA.Provo1.GroupWise	Disabled
Provo2	MTA.Provo2.GroupWise	Disabled

The eDirectory User Synchronization Configuration dialog box lists all domains in your GroupWise system, the MTA currently assigned to provide eDirectory user synchronization for each domain, and the current status of that agent's ability to perform eDirectory user synchronization.

2 Click Configure Agents.



Configure Agents

For an agent to be able to perform eDirectory user synchronization, it must both be enabled and be able to access eDirectory. Select an agent and use the buttons below to change these settings.

Agents:

Agent	State	eDirectory Access
MTA.Provo1.GroupWise	Disabled	Yes

Sets the necessary properties and rights to allow the selected agents to authenticate to eDirectory. If an agent is reporting that it cannot access eDirectory, you should run Set Up eDirectory Access and restart the agent.

Only domains with NetWare MTAs or Linux MTAs should be listed, because eDirectory user synchronization is not supported by the Windows MTA.

If domains on Windows servers are listed:

2a Cancel out of the eDirectory user synchronization dialog boxes.

2b Browse to and right-click a misconfigured MTA, then click Properties.

2c In the Platform field, select the platform where the MTA is running.

2d Click OK to save the correct platform information.

2e Return to Tools > GroupWise System Operations > eDirectory User Configuration > Configure Agents.

3 Select the NetWare MTA that you want to perform eDirectory user synchronization.

4 If the eDirectory Access column for that NetWare displays Yes, click Enable.

or

If the eDirectory Access column for that NetWare MTA displays No:

4a Click Set Up eDirectory Access.

4b Browse to and select the NetWare server where the MTA runs.

4c Click OK.

The eDirectory Access column for that NetWare MTA should now display Yes so that you can enable it.

5 Select a Linux MTA that you want to perform eDirectory user synchronization.

6 If the eDirectory Access column for that Linux MTA displays Yes, click Enable.

or

If the eDirectory Access column for that Linux MTA displays No:

6a Click Set Up eDirectory Access.

6b In the Available LDAP Servers list, select the LDAP server that you want the MTA to log into in order to gain access to eDirectory, then click Set Preferred.

6c In the LDAP User Name field, browse to and select the user that the MTA can use to log in as.

The selected user must have rights to browse properties of User objects.

Click Set Password, provide the password associated with the user selected above, then click Set Password.

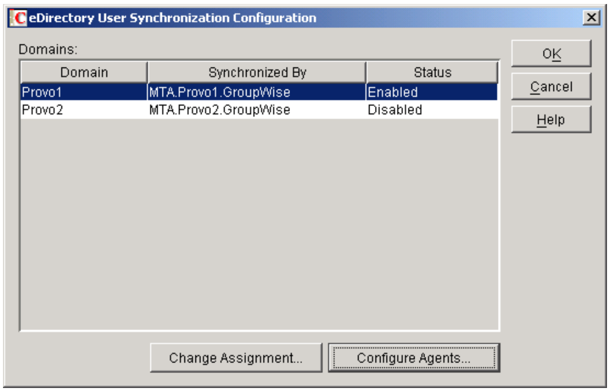
6d Click OK to save the LDAP information.

The eDirectory Access column for that Linux MTA should now display Yes so that you can enable it.

7 If your GroupWise system spans multiple trees, repeat Step 3 through Step 6 as needed to enable eDirectory user synchronization for at least one MTA in each tree.

8 Click OK to return to the eDirectory User Synchronization Configuration dialog box.

Each domain for which you have configured the MTA for eDirectory user synchronization should now display Enabled in the Status column.



Domains:

Domain	Synchronized By	Status
Provo1	MTA.Provo1.GroupWise	Enabled
Provo2	MTA.Provo2.GroupWise	Disabled

9 If all domains are now enabled, click OK to return to main ConsoleOne window, then continue with "Scheduling eDirectory User Synchronization" on page 602.

or

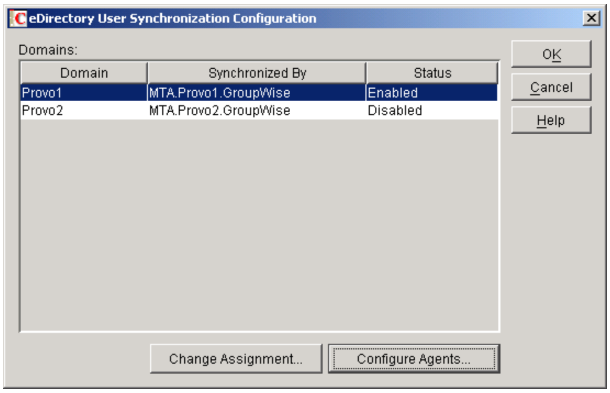
If some domains are still disabled, continue with "Assigning an eDirectory-Enabled MTA to Synchronize Other Domains" on page 601.

Assigning an eDirectory-Enabled MTA to Synchronize Other Domains

After at least one MTA is performing eDirectory user synchronization, other MTAs not performing eDirectory user synchronization themselves can have an eDirectory-enabled MTA gather the eDirectory information for them.

In the eDirectory User Synchronization Configuration dialog box,

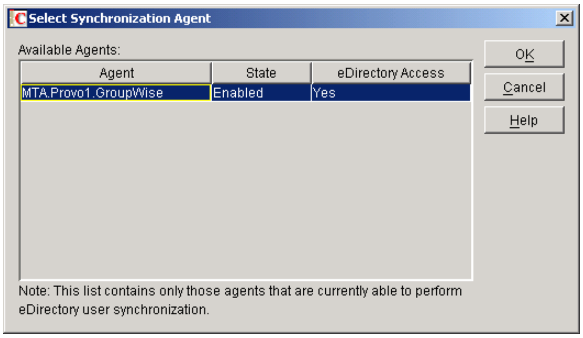
1 Click a domain that still displays Disabled in the Status column.



Domains:

Domain	Synchronized By	Status
Provo1	MTA.Provo1.GroupWise	Enabled
Provo2	MTA.Provo2.GroupWise	Disabled

2 Select an agent, then click Change Assignment.



Available Agents:

Agent	State	eDirectory Access
MTA.Provo1.GroupWise	Enabled	Yes

Note: This list contains only those agents that are currently able to perform eDirectory user synchronization.

3 Select the MTA you want to perform eDirectory user synchronization for the selected domain, then click Select.

The domain should now display Enabled in the Status column of the eDirectory User Synchronization Configuration dialog box.

4 Repeat Step 1 through Step 3 until all domains in your GroupWise system are enabled for eDirectory user synchronization.

5 Click OK to return to the main ConsoleOne window.

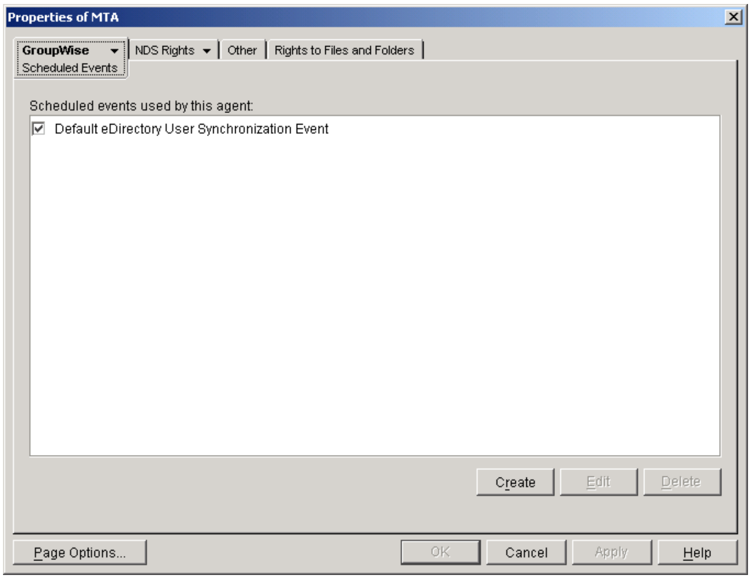
Scheduling eDirectory User Synchronization

After eDirectory user synchronization is enabled, you can perform eDirectory user synchronization at any time from the NetWare MTA agent console. See "Performing eDirectory User Synchronization" on page 615. In addition, you must create one or more eDirectory user synchronization events to cause eDirectory user synchronization to be performed on a regular basis.

To schedule an eDirectory user synchronization event:

1 In ConsoleOne, browse to and right-click the MTA object, then click Properties.

2 Click GroupWise > Scheduled Events to display the Scheduled Events page.



Scheduled events used by this agent:

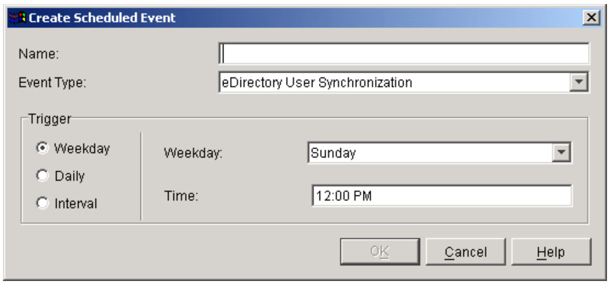
☑ Default eDirectory User Synchronization Event

The Scheduled Events page lists a pool of MTA events available to all MTAs in your GroupWise system if any events have already been created.

3 Select an existing eDirectory user synchronization event, then click Edit.

or

Click Create, then type a name for the event.



Create Scheduled Event

Name:

Event Type: eDirectory User Synchronization

Trigger

● Weekday
○ Daily
○ Interval

Weekday: Sunday

Time: 12:00 PM

4 Set Type to eDirectory User Synchronization.

5 In the Trigger box, specify when you want the eDirectory user synchronization event to take place.

You can have the synchronization event take place once a week, once a day, or at any other regular interval, at whatever time you choose.

6 Specify the time of day when you want eDirectory user synchronization to take place.

7 Click OK twice to close the scheduled event dialog boxes and save the eDirectory user synchronization event.

ConsoleOne then notifies the MTA to restart so the eDirectory user synchronization event can be put into effect.

Enabling MTA Message Logging

Message logging is turned off by default, because it causes the MTA to use additional CPU and disk resources. However, gathering information about message traffic on your GroupWise system lets you perform many valuable tasks, including:

- Tracking messages
- Gathering statistics to help optimize your GroupWise system
- Billing customers for messages delivered
- Tracking messages from the MTA Web console and from GroupWise Monitor

When you enable MTA message logging, the MTA stores data about GroupWise message traffic as it processes messages. The stored data is then available for use by the MTA Web console Message Tracking feature and by the GroupWise Monitor Message Tracking Report option. In addition, third-party programs can produce customized billing, tracking, and statistical reports based on the information stored in the database.

To enable MTA message logging:

1 In ConsoleOne, browse to and right-click the MTA object, then click Properties.

2 Click GroupWise > Message Log Settings.

3 Select a logging level to turn message logging on.

4 Specify the full path of the file where the MTA will record the logging information.

5. Specify the number of days to retain reports on disk. Reports will be automatically deleted after the specified time has passed.
6. Click OK to save the MTA message log settings.

   ConsoleOne then notifies the MTA to restart so the new settings can be put into effect.

Corresponding Startup Switches

You could also use the /messagelogsettings, /messagelogpath, /messagelogdays, and /messagelogmaxsize switches in the MTA startup file to configure MTA message logging.

MTA Web Console

For instructions on tracking messages after message logging is enabled, see "Tracking Messages" on page 623 and "Message Tracking Report" on page 934.

44 Monitoring the MTA

By monitoring the MTA, you can determine whether or not its current configuration is meeting the needs of your GroupWise® system. You have a variety of resources to help you monitor the operation of the MTA:

- "Using the MTA Agent Console" on page 605
- "Using the MTA Web Console" on page 617
- "Using MTA Log Files" on page 625
- "Using GroupWise Monitor" on page 626
- "Using NetWare 6.5 Remote Manager" on page 626
- "Using SNMP Monitoring Programs" on page 627
- "Notifying the Domain Administrator" on page 632
- "Using the MTA Error Message Documentation" on page 632
- "Employing MTA Troubleshooting Techniques" on page 633
- "Using Platform-Specific MTA Monitoring Tools" on page 633
- "Using MTA Message Logging" on page 633

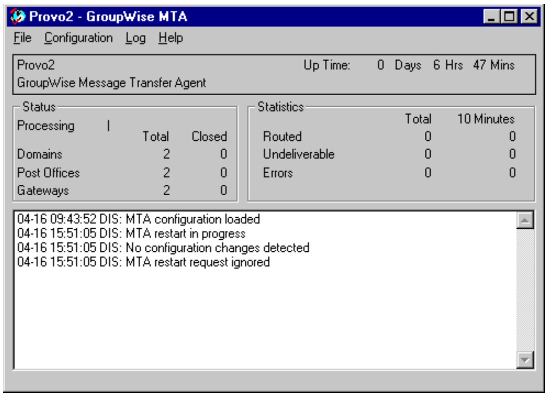
Using the MTA Agent Console

The following topics help you monitor and control the MTA from the MTA agent console:

- "Monitoring the MTA from the MTA Agent Console" on page 605
- "Controlling the MTA from the MTA Agent Console" on page 608

Monitoring the MTA from the MTA Agent Console

The MTA agent console provides information, status, and message statistics about the MTA to help you assess its current functioning.



Provo2
GroupWise Message Transfer Agent

Up Time: 0 Days 6 Hrs 47 Mins

Status

Processing |

	Total	Closed
Domains	2	0
Post Offices	2	0
Gateways	2	0

Statistics

	Total	10 Minutes
Routed	0	0
Undeliverable	0	0
Errors	0	0

```
04-16 09:43:52 DIS: MTA configuration loaded
04-16 15:51:05 DIS: MTA restart in progress
04-16 15:51:05 DIS: No configuration changes detected
04-16 15:51:05 DIS: MTA restart request ignored
```

Linux Note: You must use the --show startup switch in order to display the Linux MTA agent console. See "Starting the Linux MTA" on page 570.

Windows Note: You can suppress the Windows MTA agent console by running the Windows MTA as a service. See "Starting the Windows MTA" on page 571.

The MTA agent console consists of several components:

- "MTA Information Box" on page 606
- "MTA Status Box" on page 607
- "MTA Statistics Box" on page 607
- "MTA Alert Box" on page 607
- "MTA Admin Thread Status Box" on page 608

Do not exit the MTA agent console unless you want to stop the MTA.

NetWare Note: At a NetWare® server console, you can use Alt+Esc to change screens. In a remote console window, you can use Alt+F1 to select a screen to view. Use these keystrokes to change screens without stopping the MTA. You can use these keystrokes to display the MTA agent console if it is not immediately visible on the NetWare console.

Linux Note: On a Linux server, you can minimize the MTA agent console, but do not close it unless you want to stop the MTA.

Windows Note: On a Windows server, you can minimize the MTA agent console window, but do not close it unless you want to stop the MTA.

MTA Information Box

The MTA Information box identifies the MTA whose MTA agent console you are viewing, which is especially helpful when multiple MTAs are running on the same server.

Domain: Displays the name of the domain serviced by this MTA.

Description: Displays the description provided in the Description field in the MTA Information page in ConsoleOne®. If multiple administrators work at the server where the MTA runs, the description could include a note about who to contact before stopping the MTA.

Up Time: Displays the length of time the MTA has been running.

MTA Web Console
The Status page also displays this information.

MTA Status Box

The MTA Status box displays the current status of the MTA and its backlog.

Processing: Displays a rotating bar when the MTA is running. If the bar is not rotating, the MTA has stopped. For assistance, see "Message Transfer Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Domains: Displays the total number of domains the MTA links to and the number that are currently closed.

Post Offices: Displays the total number of post offices in the domain and the number that are currently closed.

Gateways: Displays the total number of gateways in the domain and the number that are currently closed.

If you have closed domains, post offices, or gateways, see "MTA Status Box Shows a Closed Location" in "Message Transfer Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems* for assistance.

MTA Web Console
The Status page also displays this information. In addition, you can display detailed information about specific queue contents.

MTA Statistics Box

The MTA Statistics box displays the total statistics for the current up time, and 10-minute statistics for all messages the MTA has routed.

Routed: Displays the number of messages successfully routed to the domains, post offices, and gateways serviced by the MTA.

Undeliverable: Displays the number of messages that could not be delivered to a domain, post office, or gateway. For assistance, see "MTA Statistics Box Shows Undeliverable Messages" in "Message Transfer Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Errors: Displays the number of errors the MTA encounters while processing messages in its input queues. For assistance, see "MTA Statistics Box Shows Errors" n "Message Transfer Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

MTA Web Console
The Status page also displays this information.

MTA Alert Box

The MTA Alert box displays important messages that could require an administrator's attention.

Informational Status Messages

When you first start the MTA, you typically see a message informing you the MTA configuration has been loaded.

Error Messages

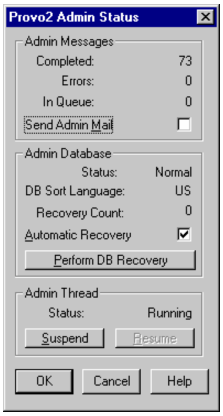
If the MTA encounters a problem that disrupts the flow of GroupWise messages, it displays an error message in the alert box. For assistance, see "Message Transfer Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

MTA Web Console
The Status page also displays this information. In addition, you can view and search MTA log files on the Log Files page.

MTA Admin Thread Status Box

The MTA admin thread updates the domain database (wpdomain.db) when domains, post offices, users, and other types of object information are added, modified, or removed, and repairs it when damage is detected.

To display the MTA Admin Thread Status box from the MTA agent console, click Configuration > Admin Status.


Provo2 Admin Status

Admin Messages
Completed: 73
Errors: 0
In Queue: 0
Send Admin Mail □

Admin Database
Status: Normal
DB Sort Language: US
Recovery Count: 0
Automatic Recovery ☑

Admin Thread
Status: Running

The following tasks pertain specifically to the MTA admin thread:

- "Suspending/Resuming the MTA Admin Thread" on page 611
- "Displaying MTA Admin Thread Status" on page 613
- "Recovering the Domain Database Automatically or Immediately" on page 614
- "Performing eDirectory User Synchronization" on page 615

MTA Web Console
You can display MTA admin thread status on the Configuration page. Under the General Settings heading, click Admin Task Processing. You can also change the admin settings for the current MTA session.

Controlling the MTA from the MTA Agent Console

You can perform the following tasks to monitor and control the MTA from the MTA agent console at the server where the MTA is running:

- "Stopping the MTA" on page 609
- "Restarting the MTA" on page 610
- "Suspending/Resuming MTA Processing for a Location" on page 610

Stopping the MTA

You might need to stop and restart the MTA for the following reasons:

- Updating the agent software
- Troubleshooting message flow problems
- Backing up the domain database
- Rebuilding the domain database

To stop the MTA from the MTA agent console:

1 Click File > Exit > Yes to stop the MTA.

NetWare Note: Use Exit (F7). If the MTA does not respond to Exit, you can use the unload command to stop the MTA. However, this might not allow the MTA to shut down gracefully. In addition, the unload command would stop all MTAs running on the server.

Linux Note: If the Linux MTA does not respond to Exit, you can kill the MTA process, as described below, but include the -9 option.

Windows Note: If the Windows MTA does not respond to Exit, you can close the MTA agent console to stop the MTA or use the Task Manager to terminate the MTA task.

2 Restart the MTA. See "Starting the MTA" on page 568.

To stop the MTA on Linux when it is running in the background as a daemon:

1 Make sure you are logged in as root.

2 If you started the Linux MTA using the grpwise script:

2a Change to the /etc/init.d directory.

2b Enter the following command:

```
./grpwise stop
```

2c Skip to Step 4

3 If you started the Linux MTA manually (not using the grpwise script):

3a Determine the process IDs (PIDs) of the MTA:

```
ps -eaf | grep gwmta
```

The PIDs for all gwmta processes are listed.

You can also obtain this information from the Environment page of the MTA Web console.

3b Kill the first MTA process listed:

Syntax:
```
kill PID
```

Example:
```
kill 1483
```

It might take a few seconds for all MTA processes to terminate.

4 Use the ps command to verify that the MTA has stopped.

```
ps -eaf | grep gwmta
```

Restarting the MTA

Restarting the MTA from the MTA agent console causes it to reread the configuration information provided in ConsoleOne. However, the MTA does not reread its startup file when you restart it from the MTA agent console.

1 At the server where the MTA is running, display the MTA agent console.

2 Click File > Restart > Yes to restart the MTA.

NetWare Note: Use Restart (F6).

If you want the MTA to reread its startup file, you must stop it, then restart it.

MTA Web Console
You can restart the MTA from the Status page. Click Restart MTA in the upper right corner of the page.

Suspending/Resuming MTA Processing for a Location

You can cause the MTA to stop processing messages for a location without stopping the MTA completely. For example, you could suspend message processing for a post office while backing up the post office.

To suspend the MTA for a location:

1 At the server where the MTA is running, display the MTA agent console.

2 Click Configuration > Status.

3 Click the location (or multiple locations) to suspend, then click Suspend.

NetWare Note: Use Options (F10) > Configuration Status. Select the location, then click Suspend.

Routing of all messages to and from the location will remain suspended until you resume processing.

To resume the MTA for a location:

1 At the server where the MTA is running, display the MTA agent console.

2 Click Configuration > Status.

3 Click the location (or multiple locations) to resume, then click Resume.

NetWare Note: Use Options (F10) > Configuration Status. Select the location, then click Resume.

MTA Web Console
You can suspend and resume processing for a specific location on the Links page. Select one or more locations, then click Suspend or Resume as needed.

Suspending/Resuming the MTA Admin Thread

You can cause the MTA to stop updating the domain database (wpdomain.db) without stopping the MTA completely. For example, you could suspend the MTA admin thread while backing up the domain database.

To suspend the MTA admin thread:

1 At the server where the MTA is running, display the MTA agent console.

2 Click Configuration > Admin Status > Suspend.

NetWare Note: Use Options > Admin Status > Suspend.

The MTA admin thread will no longer access the domain database until you resume processing.

To resume the MTA admin thread:

1 At the server where the MTA is running, display the MTA agent console.

2 Click Configuration > Admin Status > Resume.

NetWare Note: Use Options (F10) > Admin Status > Resume.

MTA Web Console
You can suspend and resume the MTA admin thread from the Configuration page. Under the General Settings heading, click Admin Task Processing > Suspend or Resume > Submit.

Displaying the MTA Software Date

It is important to keep the MTA software up-to-date. You can display the date of the MTA software from the MTA agent console.

1 At the server where the MTA is running, display the MTA agent console.

2 Click Help > About MTA.

NetWare Note: To check the date of the MTA NLM, you can list the gwmta.nlm file in the agent installation directory (typically, the sys:\system directory) or use the `modules gwmta.nlm` command at the server console prompt.

MTA Web Console
You also check the MTA software date on the Environment page.

Displaying the Current MTA Settings

You can list the current configuration settings of the MTA at the MTA agent console.

To display the current MTA settings:

1 At the server where the MTA is running, display the MTA agent console.

2 Click Configuration > Agent Settings.

NetWare Note: Use View Log File (F9) to check the MTA settings recorded at the top of the log file.

For information about the MTA settings, see Chapter 46, “Using MTA Startup Switches,” on page 643.

MTA Web Console
You check the current MTA settings on the Configuration page.

Displaying MTA Status Information

The MTA agent console displays essential information about the functioning of the MTA. More detailed information is also available.

To display detailed MTA configuration information:

1 At the server where the MTA is running, display the MTA agent console.

2 Click Configuration > Status to display a list of the locations to which the MTA is connected.

NetWare Note: Use Options (F10) > Configuration Status.

The following information is provided:

Location Name: Displays the name of the location serviced by the MTA.

Location Type: Indicates whether the location is a domain, post office, or gateway.

Connection Status: Indicates whether the MTA has been successful in locating and opening the database in the location.

- **Open:** The MTA can access the database or communicate with the agent at the location.
- **Closed:** The MTA cannot access the database or communicate with the agent at the location. For assistance, see “MTA Configuration Status Isn't Open” in n “Message Transfer Agent Problems” in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.
- **Suspended:** The MTA is not processing messages for the location because it has been suspended. See “Suspending/Resuming MTA Processing for a Location” on page 610.
- **Open Pending:** Post offices in the domain are in the process of opening and the MTA is clearing its holding queues. After this is accomplished, the MTA begins processing current messages and the status changes to Open.

Home: Displays the full path to the database that the MTA services in the listed location. For a TCP/IP connection, it displays the IP address of the server that the MTA connects to in order to service the database.

3 Select a location, then click Details to display the above information plus the following additional details:

Hold: Displays the full path to the location of the mslocal directory structure used by the MTA to hold messages for closed locations.

Pull: Displays the transfer pull directory, if any. See “Using a Transfer Pull Configuration” on page 596.

Version: Provides the version (6.*x*/5.*x*/4.*x*) of the database at the location.

Last Closed/Opened: Provides the date and time when the location was last closed and opened.

Last Closure Reason: Indicates why a closed location is closed. To look up last closure reasons, see "Message Transfer Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

Messages Written/Read: Provides statistics about throughput since the MTA was last started.

Applications: Displays the programs the MTA can deliver messages to. Depending on the configuration of your GroupWise system, you might see GroupWise agents or GroupWise 4.1 servers listed.

TCP/IP: Lists the IP port the MTA listens on.

MTA Web Console
You can check the current MTA status on the Links page at the MTA Web console. Click a direct link to view its message queues.

Displaying Live Remote Status

You can monitor the live remote connections the MTA is servicing for Remote client users. For information about live remote processing, see "Enabling Live Remote" on page 589.

1. At the server where the MTA is running, display the MTA agent console.
2. Click Configuration > Live Remote Status.

   NetWare Note: Use Options (F10) > Live Remote Status.

   The status information lists the GroupWise Remote client users who are connected to the MTA, along with the post offices and domains the MTA communicates with.

Displaying MTA Admin Thread Status

Status information for the MTA admin thread is displayed in a separate dialog box, rather than on the main MTA agent console.

To display MTA admin thread status information:

1. At the server where the MTA is running, display the MTA agent console.
2. Click Configuration > Admin Status.

   NetWare Note: Use Options (F10) > Admin Status.

   The following status information is displayed:

   Admin Message Box
   The Admin Message box provides the following information about the workload of the MTA admin thread:

   Completed: Number of administrative message successfully processed.

   Errors: Number of administrative messages not processed due to errors.

   In Queue: Number of administrative messages waiting in the queue to be processed.

   Send Admin Mail: Select this option to send a message to the administrator whenever a critical error occurs. See "Notifying the Domain Administrator" on page 632.

   Admin Database Box
   The Admin Database box provides the following information about the domain database:

   Status: Displays one of the following statuses:

- **Normal:** The MTA admin thread is able to access the domain database normally.
- **Recovering:** The MTA admin thread is recovering the domain database.
- **DB Error:** The MTA admin thread has detected a critical database error. The domain database (wpdomain.db) cannot be recovered. Rebuild the domain database in ConsoleOne. See "Rebuilding Domain or Post Office Databases" on page 349.

  The MTA admin thread will not process any more administrative messages until the database status has returned to Normal.
- **Unknown:** The MTA admin thread cannot determine the status of the domain database. Exit the MTA, then restart it, checking for errors on startup.

DB Sort Language: Displays the language code for the language that determines the sort order of lists displayed in ConsoleOne and the GroupWise system Address Book.

Recovery Count: Displays the number of recoveries performed on the domain database for the current MTA session.

Admin Thread Box
The Admin Thread box provides the following information about the MTA admin thread:

Status: Displays one of the following statuses:

- **Running:** The MTA admin thread is active.
- **Suspended:** The MTA admin thread is not processing administrative messages.
- **Starting:** The MTA admin thread is initializing.
- **Terminated:** The MTA admin thread is not running.

MTA Web Console
You can display MTA admin thread status from the Configuration page. Under the General Settings heading, click Admin Task Processing.

Recovering the Domain Database Automatically or Immediately

The MTA admin thread can recover the domain database (wpdomain.db) when it detects a problem.

To enable/disable automatic domain database recovery:

1. At the server where the MTA is running, display the MTA agent console.
2. Click Configuration > Admin Status > Automatic Recovery to toggle this feature on or off for the current MTA session.

   NetWare Note: Use Options (F10) > Admin Status > Automatic Recovery.

To recover the domain database immediately:

1. At the server where the MTA is running, display the MTA agent console.
2. Click Configuration > Admin Status > Perform DB Recovery.

   NetWare Note: Use Options (F10) > Admin Status > Perform DB Recovery.

For additional database repair procedures, see Chapter 26, "Maintaining Domain and Post Office Databases," on page 345.

MTA Web Console
You can recover the post office database from the Configuration page. Under the General Settings heading, click Admin Task Processing. Select Automatic Recovery or Perform DB Recovery as needed.

Performing eDirectory User Synchronization

You can configure the MTA to perform Novell® eDirectory™ user synchronization at regular intervals. See "Using eDirectory User Synchronization" on page 598. You can also start eDirectory user synchronization manually from the NetWare MTA agent console.

To start eDirectory user synchronization immediately:

1 At the server where the NetWare MTA is running, display the MTA agent console.

2 Press F4.

MTA Web Console
You can see when the next eDirectory user synchronization even will occur at the bottom of the Configuration page.

Browsing the Current MTA Log File

The MTA displays only the most urgent messages in the alert box. Additional information is written to the MTA log file. The amount of information depends on the current log settings for the MTA. See "Using MTA Log Files" on page 625.

The information automatically scrolls up the screen as additional information is written. You can stop the automatic scrolling so you can manually scroll back through earlier information.

To browse the current MTA log file and control scrolling:

1 At the server where the MTA is running, display the MTA agent console.

2 Click Log > Active Log.

NetWare Note: Use View Log File (F9).

3 Deselect Automatic Scrolling to manually scroll back through parts of the log that have already scrolled out of the box.

4 Click Freeze to stop the MTA from logging information to the active log box.

5 Click Thaw when you want the MTA to resume logging information to the active log box.

For explanations of messages in the MTA log file, see "Message Transfer Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

MTA Web Console
You can browse and search MTA log files on the Log Files page.

Viewing a Selected MTA Log File

Reviewing log files is an important way to monitor the functioning of the MTA.

1 At the server where the MTA is running, display the MTA agent console.

2 Click Log > View Log Files.

3 Select a log file, then click View.

NetWare Note: Use Options (F10) > View Log Files.

For explanations of messages in the MTA log file, see "Message Transfer Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

MTA Web Console
You can view and search MTA log files on the Log Files page.

Cycling the MTA Log File

You can have the MTA start a new log file as needed.

1. At the server where the MTA is running, display the MTA agent console.
2. Click Log > Cycle Log.

   NetWare Note: Use Options (F10) > Cycle Log File.

Adjusting MTA Log Settings

Default log settings are established when you start the MTA. However, they can be adjusted for the current MTA session from the MTA agent console.

1. At the server where the MTA is running, display the MTA agent console.
2. Click Log > Log Settings.

   NetWare Note: Use Options (F10) > Log Settings.
3. Adjust the values as needed for the current MTA session.

See "Using MTA Log Files" on page 625.

MTA Web Console
You can adjust MTA log settings from the Configuration page. Click the Event Log Settings heading.

Editing the MTA Startup File

You can change the configuration of the MTA by editing the MTA startup file from the MTA agent console.

1. At the server where the MTA is running, display the MTA agent console.
2. Click Configuration > Edit Startup File.

   NetWare Note: Use Options > Actions > Edit Startup File.
3. Make the necessary changes, then save and exit the startup file.
4. Stop and restart the MTA.

Accessing Online Help for the MTA

Click Help on the menu bar for information about the MTA agent console. Click the Help button in any dialog box for additional information.

NetWare Note: Press F1 for information in any dialog box or menu.

Using the MTA Web Console

The MTA Web console enables you to monitor the MTA from any location where you have access to a Web browser and the Internet. This provides substantially more flexible access than the MTA agent console, which can only be accessed from the server where the MTA is running.

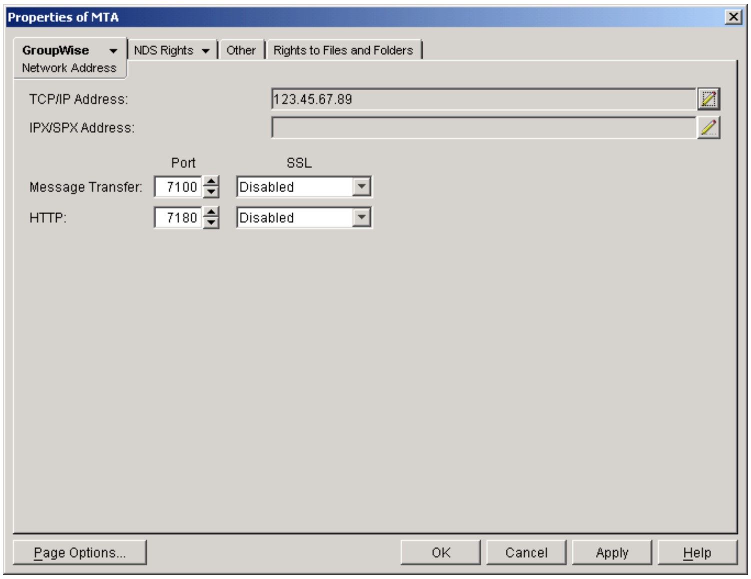
- "Setting Up the MTA Web Console" on page 617
- "Accessing the MTA Web Console" on page 619
- "Monitoring the MTA from the MTA Web Console" on page 619

Setting Up the MTA Web Console

The default HTTP port for the MTA Web console is established during MTA installation. You can change the port number and increase security after installation in ConsoleOne.

1 In ConsoleOne, browse to and right-click the MTA object, then click Properties.

2 Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 123.45.67.89

IPX/SPX Address:

	Port	SSL
Message Transfer:	7100	Disabled
HTTP:	7180	Disabled

If you configured the MTA for TCP/IP links during installation, the TCP/IP Address field should display the MTA server's network address. If it does not, follow the instructions in "Using TCP/IP Links between Domains" on page 579. The MTA must be configured for TCP/IP in order to provide the MTA Web console.

3 Make a note of the IP address or DNS hostname in the TCP/IP Address field. You will need this information to access the MTA Web console.

The HTTP Port field displays the default port number of 7180.

4 If the default HTTP port number is already in use on the MTA server, specify a unique port number.

5 Make a note of the HTTP port number. You will need this information to access the POA Web console.

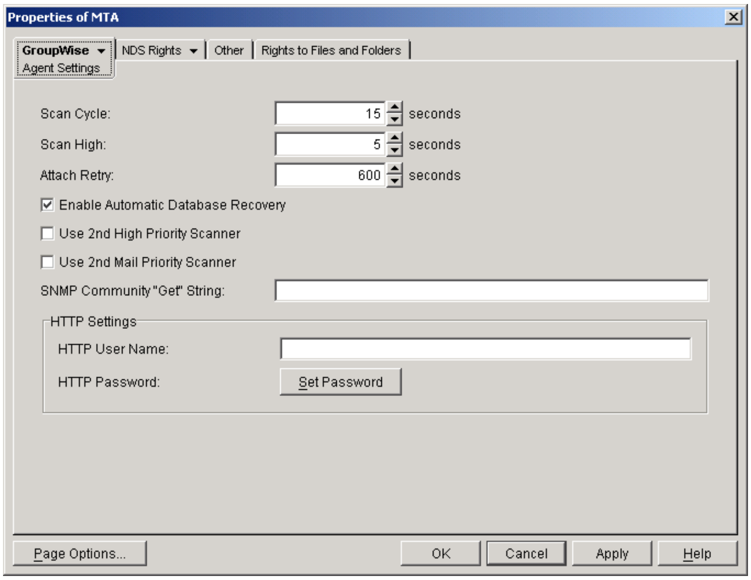
6 If you want to use an SSL connection for the MTA Web console, select Enabled in the HTTP SSL drop-down list.

For additional instructions about using SSL connections, see Chapter 80, “Encryption and Certificates,” on page 1039.

7 Click Apply to save your changes on the Network Address page.

If you want to limit access to the MTA Web console, you can provide a username and password.

8 Click GroupWise > Agent Settings to display the Agent Settings age.



Scan Cycle: 15 seconds

Scan High: 5 seconds

Attach Retry: 600 seconds

☑ Enable Automatic Database Recovery

□ Use 2nd High Priority Scanner

□ Use 2nd Mail Priority Scanner

SNMP Community "Get" String:

HTTP Settings

HTTP User Name:

HTTP Password:

9 In the HTTP Settings box:

9a In the HTTP User Name field, specify a unique username.

9b Click Set Password.

9c Type the password twice for verification.

9d Click Set Password.

Unless you are using an SSL connection, do not use an eDirectory username and password because the information passes over the insecure connection between your Web browser and the MTA.

For convenience, use the same username and password for all agents that you plan to monitor from GroupWise Monitor. This saves you from having to provide the username and password information as Monitor accesses each agent.

10 Click OK to save the MTA Web console settings.

ConsoleOne then notifies the MTA to restart so the new settings can be put into effect.

Corresponding Startup Switches

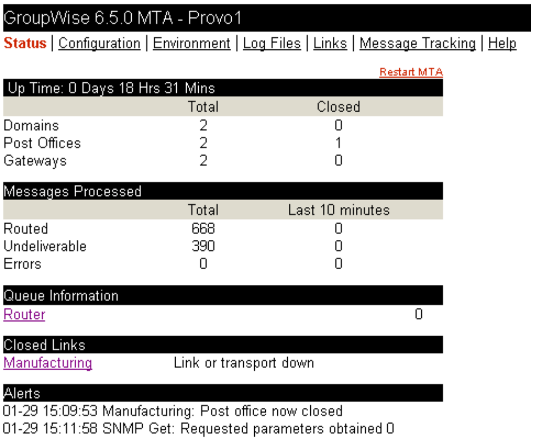
You could also use the /httpport, /httpuser, and /httppassword startup switches in the MTA startup file to enable the MTA Web console. In addition, you can use the /httprefresh switch to control how often the MTA refreshes the information provided to your Web browser.

Accessing the MTA Web Console

To monitor the MTA from your Web browser, view the MTA Web console by supplying the network address and port number as provided in ConsoleOne. For example:

http://123.456.78.90:7100
http://123.456.78.90:7180
http://server1:7100
https://server2:7180

When viewing the MTA Web console, you can specify either the message transfer port or the HTTP port.


Status | Configuration | Environment | Log Files | Links | Message Tracking | Help
Restart MTA

GroupWise 6.5.0 MTA - Provo1

Up Time: 0 Days 18 Hrs 31 Mins

	Total	Closed
Domains	2	0
Post Offices	2	1
Gateways	2	0

Messages Processed

	Total	Last 10 minutes
Routed	668	0
Undeliverable	390	0
Errors	0	0

Queue Information

Router	0

Closed Links

Manufacturing	Link or transport down

Alerts

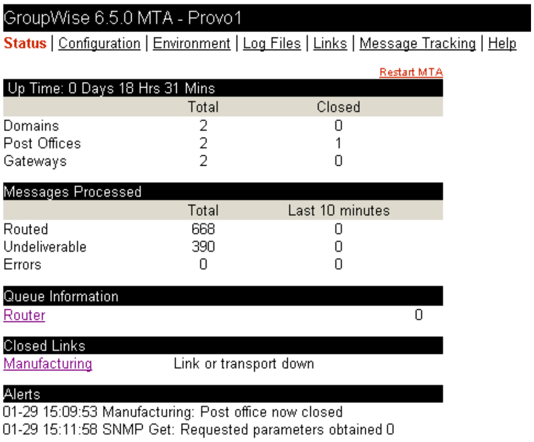
01-29 15:09:53 Manufacturing: Post office now closed
01-29 15:11:58 SNMP Get: Requested parameters obtained 0

Monitoring the MTA from the MTA Web Console

The MTA Web console provides several pages of information to help you monitor the performance of the MTA. The bar at the top of the MTA Web console displays the name of the MTA and its domain. Below this bar appears the MTA Web console menu that lists the pages of information available in the MTA Web console. Online help throughout the MTA Web console helps you interpret the information being displayed and use the links provided.

Monitoring MTA Status

When you first access the MTA Web console, the Status page is displayed. Online help throughout the MTA Web console helps you interpret the information being displayed and use the links provided.



GroupWise 6.5.0 MTA - Provo1

Status | Configuration | Environment | Log Files | Links | Message Tracking | Help
Restart MTA

Up Time: 0 Days 18 Hrs 31 Mins

	Total	Closed
Domains	2	0
Post Offices	2	1
Gateways	2	0

Messages Processed

	Total	Last 10 minutes
Routed	668	0
Undeliverable	390	0
Errors	0	0

Queue Information

Router	0

Closed Links

Manufacturing	Link or transport down

Alerts

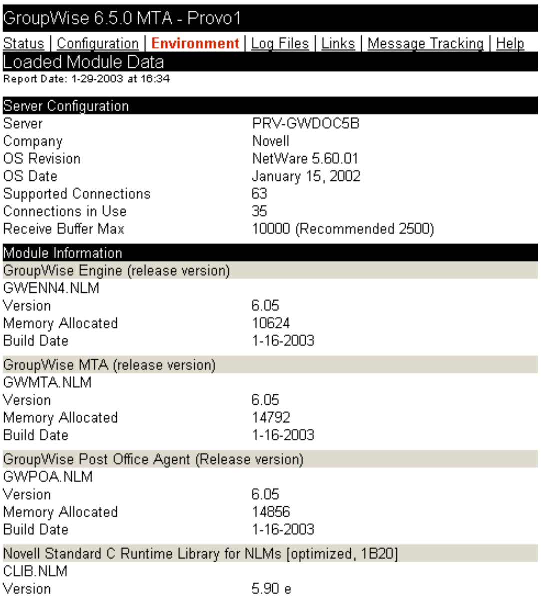
01-29 15:09:53 Manufacturing: Post office now closed
01-29 15:11:58 SNMP Get: Requested parameters obtained 0

Click the Router link to display details about the MTA routing queue (gwinprog). You can quickly determine how many messages are awaiting processing, how large they are, and how long they have been waiting in the routing queue.

Click a closed location to display is holding queue to see how many messages are waiting for transfer.

Checking the MTA Operating System Environment

On the MTA Web console menu, click Environment to display information about the operating system where the MTA is running. On a NetWare server, the following information is displayed:



GroupWise 6.5.0 MTA - Provo1

Status | Configuration | Environment | Log Files | Links | Message Tracking | Help

Loaded Module Data

Report Date: 1-29-2003 at 16:34

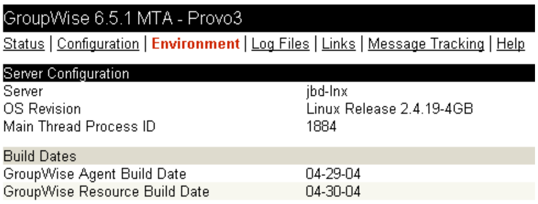
Server Configuration

Server	PRV-GWDOC5B
Company	Novell
OS Revision	NetWare 5.60.01
OS Date	January 15, 2002
Supported Connections	63
Connections in Use	35
Receive Buffer Max	10000 (Recommended 2500)

Module Information

GroupWise Engine (release version)	
GWENN4.NLM	
Version	6.05
Memory Allocated	10624
Build Date	1-16-2003
GroupWise MTA (release version)	
GWMTA.NLM	
Version	6.05
Memory Allocated	14792
Build Date	1-16-2003
GroupWise Post Office Agent (Release version)	
GWPOA.NLM	
Version	6.05
Memory Allocated	14856
Build Date	1-16-2003
Novell Standard C Runtime Library for NLMs [optimized, 1B20]	
CLIB.NLM	
Version	5.90 e

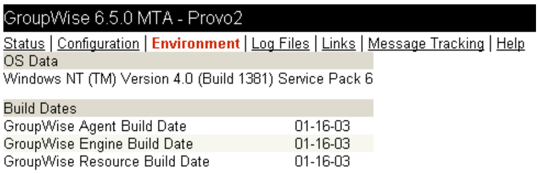
On a Linux server, the following information is displayed:


GroupWise 6.5.1 MTA - Provo3
Status | Configuration | Environment | Log Files | Links | Message Tracking | Help

Server Configuration	
Server	jbd-lnx
OS Revision	Linux Release 2.4.19-4GB
Main Thread Process ID	1884

Build Dates	
GroupWise Agent Build Date	04-29-04
GroupWise Resource Build Date	04-30-04

On a Windows server, the following information is displayed:


GroupWise 6.5.0 MTA - Provo2
Status | Configuration | Environment | Log Files | Links | Message Tracking | Help

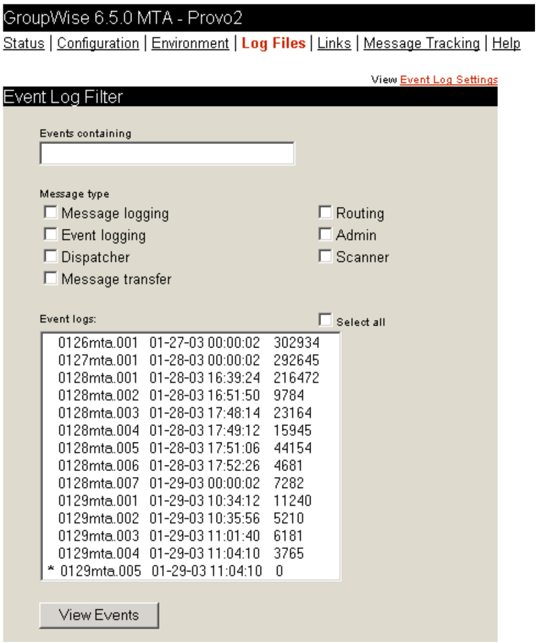
OS Data

Windows NT (TM) Version 4.0 (Build 1381) Service Pack 6

Build Dates	
GroupWise Agent Build Date	01-16-03
GroupWise Engine Build Date	01-16-03
GroupWise Resource Build Date	01-16-03

Viewing and Searching MTA Log Files

On the MTA Web console menu, click Log Files to display and search MTA log files.



```
0126mta.001  01-27-03 00:00:02  302934
0127mta.001  01-28-03 00:00:02  292645
0128mta.001  01-28-03 16:39:24  216472
0128mta.002  01-28-03 16:51:50  9784
0128mta.003  01-28-03 17:48:14  23164
0128mta.004  01-28-03 17:49:12  15945
0128mta.005  01-28-03 17:51:06  44154
0128mta.006  01-28-03 17:52:26  4681
0128mta.007  01-29-03 00:00:02  7282
0129mta.001  01-29-03 10:34:12  11240
0129mta.002  01-29-03 10:35:56  5210
0129mta.003  01-29-03 11:01:40  6181
0129mta.004  01-29-03 11:04:10  3765
* 0129mta.005  01-29-03 11:04:10  0
```

To view a particular log file, select the log file, then click View Events.

To search all log files for a particular string, type the string in the Events Containing field, select Select All, then click View Events. You can also manually select multiple log files to search.

In the Message type list, you can select one or more types of MTA processing to search for:

Message Logging (MLG): The message logging threads write information into the message log file if message logging has been turned on. See "Enabling MTA Message Logging" on page 603.

Event Logging (LOG): The event logging thread writes information into the event log files that you can search on this page. See "Using MTA Log Files" on page 625.

Dispatcher (DIS): The dispatcher thread starts other MTA threads as needed to meet the demands being put on the MTA at any given time.

Message Transfer (MTP): The message transfer threads communicate with other MTAs and with POAs in the local domain to transfer messages to domains and post offices to which the local MTA is linked by way of TCP/IP. See "Using TCP/IP Links between Domains" on page 579 and "Using TCP/IP Links between a Domain and its Post Offices" on page 583.

Router (RTR): The router threads process messages in the routing queue and prepare them for transfer to the next hop in the link path to their destinations. See "Optimizing the Routing Queue" on page 639.

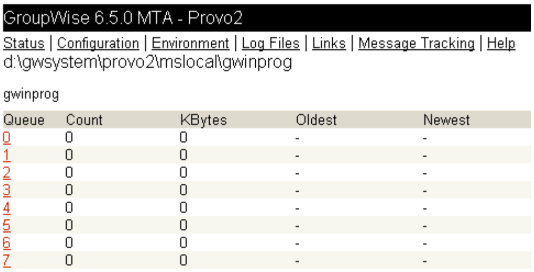
Admin (ADM): The admin thread updates the domain database (wpdomain.db) whenever administrative information changes. See "MTA Admin Thread Status Box" on page 608.

Scanner (SCA): The scanner threads check for incoming messages when UNC or mapped links are in use. See "Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices" on page 638.

The results of the search are displayed on a separate page which can be printed.

Monitoring the Routing Queue

On the MTA Web console menu, click Status, then click Router to display the contents of the routing queue. Typically, no message files are waiting unless the MTA is down or backlogged.


GroupWise 6.5.0 MTA - Provo2
Status | Configuration | Environment | Log Files | Links | Message Tracking | Help

d:\gwsystem\provo2\mslocal\gwinprog

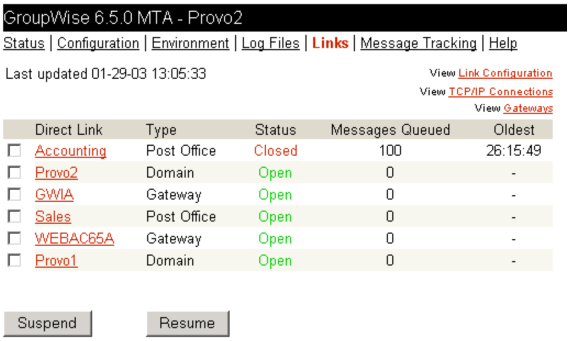
gwinprog

Queue	Count	KBytes	Oldest	Newest
0	0	0	-	-
1	0	0	-	-
2	0	0	-	-
3	0	0	-	-
4	0	0	-	-
5	0	0	-	-
6	0	0	-	-
7	0	0	-	-

You can click any queue to view the message files it contains.

Monitoring Links

On the MTA Web console menu, click Links to monitor the direct links between the MTA and other locations.


GroupWise 6.5.0 MTA - Provo2
Status | Configuration | Environment | Log Files | Links | Message Tracking | Help
View Link Configuration
View TCP/IP Connections
View Gateways
Suspend
Resume

Last updated 01-29-03 13:05:33

	Direct Link	Type	Status	Messages Queued	Oldest
□	Accounting	Post Office	Closed	100	26:15:49
□	Provo2	Domain	Open	0	-
□	GWIA	Gateway	Open	0	-
□	Sales	Post Office	Open	0	-
□	WEBAC65A	Gateway	Open	0	-
□	Provo1	Domain	Open	0	-

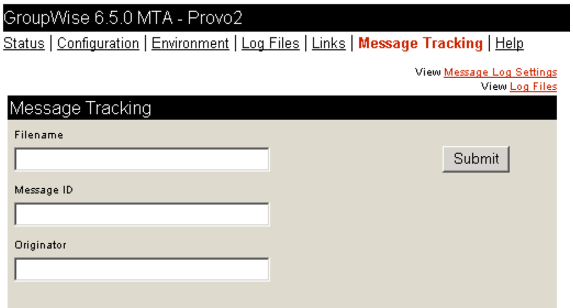
Click a location to view its holding queue. Click View Link Configuration to determine the address of each location and access the agent Web consoles of other domains and of post offices that belong to the local domain. Click View TCP/IP Connections to view incoming and outgoing TCP/IP links. Click VIew Gateways to restrict the list to just gateways.

Tracking Messages

Before you can track messages at the MTA Web console, you must enable message logging for MTAs throughout your system. See "Enabling MTA Message Logging" on page 603. When you enable MTA message logging, the MTA stores data about GroupWise message traffic as it processes messages. The stored data is then available for use from the MTA Web console.

To track a specific message, have the sender check the Sent Item Properties for the message in the GroupWise client. The Mail Envelope Properties field displays the message ID of the message; for example, 3AD5EDEB.31D : 3 : 12763. To track all messages sent by a particular user, make a note of the user's GroupWise user ID.

On the MTA Web console menu, click Message Tracking.


GroupWise 6.5.0 MTA - Provo2
Status | Configuration | Environment | Log Files | Links | Message Tracking | Help
View Message Log Settings
View Log Files
Message Tracking
Filename
Submit
Message ID
Originator

Fill in *one* of the fields, depending on what you want to track, then click Submit.The results of the search are displayed on a separate page which can be printed.

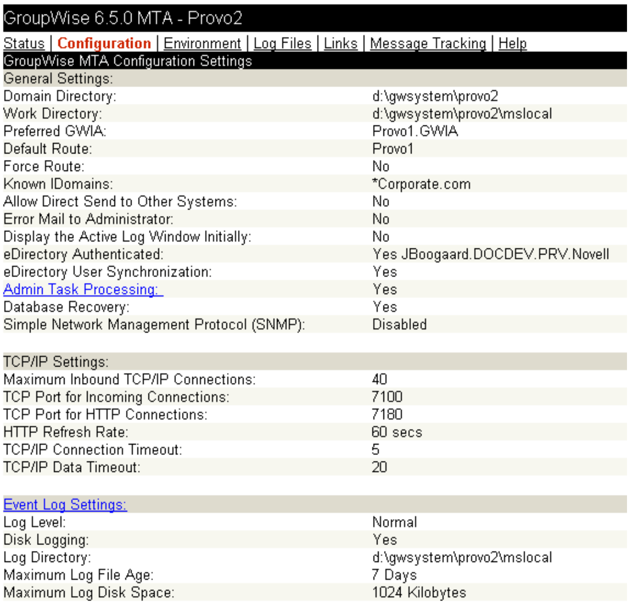
Controlling the MTA from the MTA Web Console

At the MTA Web console, you can change some MTA log settings for the current MTA session. You can also stop and start some specific MTA threads.

- "Changing MTA Configuration Settings" on page 623
- "Controlling the MTA Admin Thread" on page 624
- "Controlling Links to Other Locations" on page 624

Changing MTA Configuration Settings

On the MTA Web console menu, click Configuration. Online help on the Configuration page helps you interpret the configuration information being displayed.


Status | Configuration | Environment | Log Files | Links | Message Tracking | Help

GroupWise 6.5.0 MTA - Provo2

GroupWise MTA Configuration Settings

General Settings:	
Domain Directory:	d:\gwsystem\provo2
Work Directory:	d:\gwsystem\provo2\mslocal
Preferred GWIA:	Provo1.GWIA
Default Route:	Provo1
Force Route:	No
Known IDomains:	*Corporate.com
Allow Direct Send to Other Systems:	No
Error Mail to Administrator:	No
Display the Active Log Window Initially:	No
eDirectory Authenticated:	Yes JBoogaard.DOCDEV.PRV.Novell
eDirectory User Synchronization:	Yes
Admin Task Processing:	Yes
Database Recovery:	Yes
Simple Network Management Protocol (SNMP):	Disabled

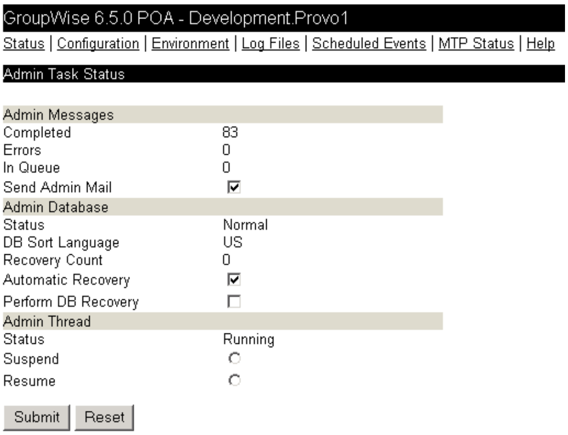
TCP/IP Settings:	
Maximum Inbound TCP/IP Connections:	40
TCP Port for Incoming Connections:	7100
TCP Port for HTTP Connections:	7180
HTTP Refresh Rate:	60 secs
TCP/IP Connection Timeout:	5
TCP/IP Data Timeout:	20

Event Log Settings:	
Log Level:	Normal
Disk Logging:	Yes
Log Directory:	d:\gwsystem\provo2\mslocal
Maximum Log File Age:	7 Days
Maximum Log Disk Space:	1024 Kilobytes

Click the Event Log Settings heading to change the MTA log settings for the current MTA session.

Controlling the MTA Admin Thread

On the Configuration page, click Admin Task Processing.


Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help
Submit
Reset

GroupWise 6.5.0 POA - Development.Provo1

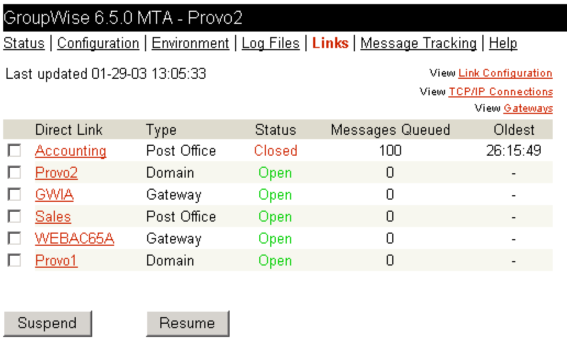
Admin Task Status

Admin Messages	
Completed	83
Errors	0
In Queue	0
Send Admin Mail	☑
Admin Database	
Status	Normal
DB Sort Language	US
Recovery Count	0
Automatic Recovery	☑
Perform DB Recovery	□
Admin Thread	
Status	Running
Suspend	○
Resume	○

Modify the functioning of the MTA admin thread as needed, then click Submit. The changes remain in effect for the current MTA session.

Controlling Links to Other Locations

On the MTA Web console menu, click Links.



GroupWise 6.5.0 MTA - Provo2

Status | Configuration | Environment | Log Files | **Links** | Message Tracking | Help

Last updated 01-29-03 13:05:33

View Link Configuration
View TCP/IP Connections
View Gateways

	Direct Link	Type	Status	Messages Queued	Oldest
□	Accounting	Post Office	Closed	100	26:15:49
□	Provo2	Domain	Open	0	-
□	GWIA	Gateway	Open	0	-
□	Sales	Post Office	Open	0	-
□	WEBAC65A	Gateway	Open	0	-
□	Provo1	Domain	Open	0	-

Select one or more locations, then click Suspend or Resume as needed.

Using MTA Log Files

Error messages and other information about MTA functioning are written to log files as well as displaying on the MTA agent console. Log files can provide a wealth of information for resolving problems with MTA functioning or message flow. This section covers the following subjects to help you get the most from MTA log files:

- "Configuring MTA Log Settings and Switches" on page 625
- "Viewing MTA Log Files" on page 626
- "Interpreting MTA Log File Information" on page 626

Configuring MTA Log Settings and Switches

The following aspects of logging are configurable:

- Log File Path (/log)
- Disk Logging (/logdiskoff)
- Logging Level (/loglevel)
- Maximum Log File Age (/logdays)
- Maximum Log File Size (/logmax)

You can configure the log settings in the following ways:

- Using ConsoleOne to establish defaults (see "Adjusting the MTA Logging Level and Other Log Settings" on page 588)
- Using startup switches to override ConsoleOne settings (see "Using MTA Startup Switches" on page 643)
- Using the MTA agent console to override other MTA settings for the current session (see "Adjusting MTA Log Settings" on page 616
- Using the MTA Web console to override other MTA settings for the current MTA session (see "Controlling the MTA from the MTA Web Console" on page 623)

Viewing MTA Log Files

You can view the contents of the MTA log file from the MTA agent console and Web console. See the following tasks:

- "Browsing the Current MTA Log File" on page 615
- "Viewing a Selected MTA Log File" on page 615
- "Cycling the MTA Log File" on page 616
- "Viewing and Searching MTA Log Files" on page 621

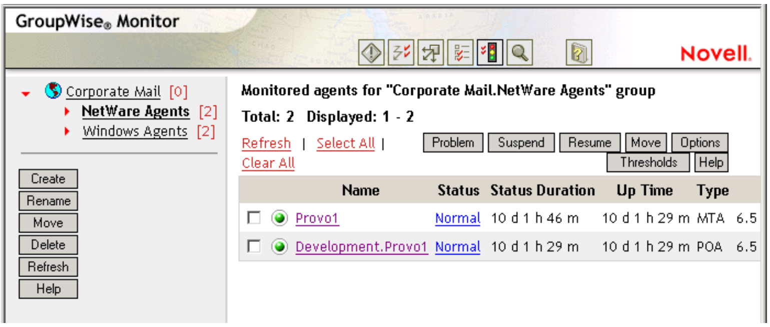
Interpreting MTA Log File Information

On startup, the MTA records the MTA settings currently in effect. Thereafter, it logs events that take place, including errors. To look up error messages that appear in MTA log files, see "Message Transfer Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

Because the MTA consists of multiple threads, you might find it useful to retrieve the log file into an editor and sort it on the thread ID that follows the date and time information. Sorting will group all messages together for the same MTA thread. At the MTA Web console, you can search through multiple log files. See "Viewing and Searching MTA Log Files" on page 621. You can also use the search capability of the MTA Web console to gather information about a specific MTA thread. See "Viewing and Searching MTA Log Files" on page 621.

Using GroupWise Monitor

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents and gateways from any location where you are connected to the Internet and have access to a Web browser. The MTA Web console can be accessed from GroupWise Monitor, enabling you to monitor all MTAs in your GroupWise system from one convenient location. In addition, GroupWise Monitor can notify you when agent problems arise.



Monitored agents for "Corporate Mail.NetWare Agents" group

Total: 2 Displayed: 1 - 2

		Name	Status	Status Duration	Up Time	Type
□	●	Provo1	Normal	10 d 1 h 46 m	10 d 1 h 29 m	MTA 6.5
□	●	Development.Provo1	Normal	10 d 1 h 29 m	10 d 1 h 29 m	POA 6.5

For installation and setup instructions, see "Installing GroupWise Monitor" in the *GroupWise 6.5 Installation Guide*. For usage instructions, see "Monitor" on page 901.

Using NetWare 6.5 Remote Manager

If the MTA is running on a NetWare 6.5 server, you can use the IP Address Management feature in NetWare Remote Manager (NetWare Remote Manager > Manage Server > IP Address Management) to view the IP address and port configuration for the MTA. This is also true for other GroupWise agents (POA, Internet Agent, and WebAccess Agent) running on NetWare 6.5 servers.

IMPORTANT: If the MTA is running in protected mode, it will not display in NetWare Remote Manager.

You access NetWare Remote Manager by entering the following URL in a Web browser:

```
http://server_address:8008
```

For example:

```
http://137.65.123.11:8008
```

For more information about using NetWare Remote Manager, see the NetWare 6.5 documentation (http://www.novell.com/documentation/nw65).

Using SNMP Monitoring Programs

You can monitor the MTA from the Management and Monitoring component of Novell ZENworks® for Servers, ManageWise®, or another SNMP management and monitoring program. When properly configured, the MTA sends SNMP traps to network management consoles for display along with other SNMP monitored programs.

Although the MTA is SNMP-enabled by default, the server where the MTA is installed must be properly configured to support SNMP, and the MTA object in eDirectory must be properly configured as well. To set up SNMP services for your server, complete the following tasks:

- "Setting Up SNMP Services for the MTA" on page 627
- "Copying and Compiling the MTA MIB File" on page 630
- "Customizing Your ManageWise Installation to Monitor the MTA" on page 631
- "Configuring the MTA for SNMP Monitoring" on page 631

Setting Up SNMP Services for the MTA

Select the instructions for the platform where the MTA runs:

- "Setting Up SNMP Services for the NetWare MTA" on page 627
- "Setting Up SNMP Services for the Linux MTA" on page 628
- "Setting Up SNMP Services for the Windows MTA" on page 628

Setting Up SNMP Services for the NetWare MTA

The NetWare MTA supports SNMP through the SNMP services loaded on the NetWare server. SNMP services are provided through the SNMP NLM. The SNMP NLM initiates and responds to requests for monitoring information and generates trap messages.

If the SNMP NLM is not loaded before the NetWare MTA, the MTA still loads and functions normally, but SNMP support is disabled. The MTA does not attempt to auto-load snmp.nlm.

To load the SNMP NLM manually:

1. Go to the console of each NetWare server where you want to implement SNMP services.

   These servers should already have the GroupWise agents installed.

2. Type the command to load the SNMP NLM:

   Syntax:

   ```
   load snmp v control=x monitor=y trap=z
   ```

where v represents Verbose, meaning to display informational messages, and *x*, *y* and *z* are replaced with your system SNMP community strings for SNMP SETs, GETs and TRAPs).

Example:

```
load snmp v control=private monitor=public      trap=all
```

The configuration for the SNMP NLM is found in snmp.cfg and traptarg.cfg in the sys:\etc directory. View the contents of these files for more information.

The TCP/IP NLM automatically loads snmp.nlm, using default values for the community strings. If your system uses different community string values, load snmp.nlm before tcpip.nlm.

3 If the SNMP NLM is already loaded, you can add the control and trap parameters by typing the following at the console prompt:

```
snmp control= trap=
```

To automatically load these commands, include them in the autoexec.ncf file.

For more information about implementing SNMP services, see your NetWare documentation.

4 Skip to "Copying and Compiling the MTA MIB File" on page 630.

Setting Up SNMP Services for the Linux MTA

The Linux MTA is compatible with NET-SNMP. An older version of SNMP called UCD-SNMP cannot be used with the Linux MTA. NET-SNMP comes standard with the versions of Red Hat Linux supported for GroupWise 6.5 for Linux, but it does not come standard with the supported versions of SUSE Linux. If you are using SUSE Linux, you must update to NET-SNMP in order to use SNMP to monitor the Linux MTA.

1 Make sure you are logged in as root.

2 If NET-SNMP is not already set up on your Linux server, use the following command to configure SNMP:

```
snmpconf -g basic_setup
```

The snmpconf command creates the snmpd.conf file in one of the following directories, depending on your version of Linux:

/usr/share/snmp
/usr/local/share/snmp
~/.snmp

3 Locate the snmpd.conf file on your Linux server.

4 In a text editor, open the snmpd.conf file and add the following line:

dlmod Gwsnmp /opt/novell/gw/agents/lib/libgwsnmp.so

5 Save the snmpd.conf file and exit the text editor.

6 Restart the SNMP daemon (snmpd) to put the changes into effect.

7 Skip to "Copying and Compiling the MTA MIB File" on page 630.

Setting Up SNMP Services for the Windows MTA

SNMP support is provided for up to eight Windows MTAs on the same Windows server. Upon startup, each instance of the MTA is dynamically assigned a row in its SNMP table. View the contents of the MTA MIB for a description of the SNMP variables in the table.

To set up SNMP services for the Windows MTA, complete the following tasks:

- "Installing Windows SNMP Support" on page 629
- "Installing GroupWise Agent SNMP Support" on page 629

Installing Windows SNMP Support

For Windows NT 3.51 and 4.0 and for Windows 2000, the SNMP service is usually not included during the initial operating system installation. The SNMP service can be easily added at any time. To add or configure the SNMP service, you must be logged in as a member of the Administrator group.

To add the SNMP service to a Windows NT server:

1. From the Control Panel, double-click Network.
2. For Windows NT 4.0, click Services > Add, then select SNMP Service.

   or

   For Windows NT 3.51, click Add Software, select TCP/IP Protocol and Related Components, then select SNMP Service.
3. Follow the on-screen prompts. You will need your original Windows NT disk.

   You are given the opportunity to configure the SNMP service. The only required information for GroupWise is the Trap Destination and Community Name.
4. After the installation is complete, reboot the server.

   For more information about configuring the SNMP service, see your Windows NT documentation.

To add the SNMP service to a Windows 2000 server:

1. From the Control Panel, double-click Add/Remove Programs.
2. Click Add/Remove Windows Components.
3. Select Management and Monitoring Tools.
4. Click Details, then select Simple Network Management Protocol.

Continue with "Installing GroupWise Agent SNMP Support" on page 629.

Installing GroupWise Agent SNMP Support

The GroupWise Agent Installation program includes an option for installing SNMP support. However, if the server where you installed the agents did not yet have SNMP set up, that installation option was not available. Now that you have set up SNMP, you can install GroupWise agent SNMP support.

At the Windows server where you want to install the GroupWise agent SNMP support:

1. Run setup.exe at the root of the *GroupWise 6.5 Administrator* CD, then click Install Products > GroupWise Agents > Install GroupWise Agents.

   or

   Run install.exe from the agents subdirectory on the *GroupWise 6.5 Administrator* CD or in your software distribution directory if you have updated it with the latest GroupWise software.
2. In the Installation Path dialog box, browse to and select the path where the agent software is installed, then select Install and Configure SNMP for GroupWise Agents.

3 To shorten the install time, deselect Install GroupWise Agent Software.

4 Continue through the rest of the installation process as prompted by the Agent Installation program.

The Agent Installation program copies the SNMP support files to the agent installation directory, makes the appropriate Windows registry entries, and restarts the Windows SNMP service.

5 Continue with "Copying and Compiling the MTA MIB File" on page 630.

Copying and Compiling the MTA MIB File

An SNMP-enabled MTA returns information contained in a Management Information Base (MIB). The MIB is an ASCII data structure that defines the information gathered. It also defines the properties that can be monitored and managed on the SNMP-enabled MTA.

Before you can monitor an SNMP-enabled MTA, you must compile the gwmta.mib file using your SNMP management program. For NetWare or Windows, the GroupWise MIBs are located on the *GroupWise 6.5 Administrator* CD in the \agents\snmp directory or in the *software_distribution_directory*\agents\snmp directory if you have updated it with the latest GroupWise software. For Linux, the GroupWise MIBS are located on the *GroupWise 6.5 for Linux Administrator* CD in the /agents/snmp directory.

1 Copy the gwmta.mib file from the \agents\snmp directory to the location required by your SNMP management program.

For example, ManageWise users would copy the gwmta.mib file to the \mw\nms\snmpmibs\current directory. ZENworks Server Management users can access the gwmta.mib file in the software distribution directory.

2 Compile or import the gwmta.mib file as required by your SNMP management program.

For example, to compile the gwmta.mib file for ZENworks Server Management:

2a In ConsoleOne, right-click the Site Server object, then click Properties > MIB Pool.

2b Click Modify Pool > Add.

2c Browse to and select the gwmta.mib file, then click OK.

2d Click Compile.

2e Make sure that the server where the MTA is running is configured to send SNMP traps to the ZENworks Server Management Site Server.

- On a NetWare server, add the IP address or hostname of the ZENworks Server Management Site Server to the traptarg.cfg file in the sys:\etc directory.
- On a Windows server, add the IP address or hostname of the ZENworks Server Management Site Server to the list of trap destinations.

  From the Windows NT Control Panel, double-click Network, or, from the Windows 2000 Control Panel, double-click Administrative Tools. Then click Services > SNMP Service > Properties > Traps.

Refer to your SNMP management program documentation for further instructions.

3. If you are using Novell ManageWise, continue with "Customizing Your ManageWise Installation to Monitor the MTA" on page 631.

   or

   If you are not using ManageWise, skip to "Configuring the MTA for SNMP Monitoring" on page 631.

Customizing Your ManageWise Installation to Monitor the MTA

The GroupWise agent installation includes files that help ManageWise monitor the GroupWise agents more effectively.

- "GroupWise MIB Files" on page 631
- "GroupWise Agent Alarm Help File" on page 631

These capabilities are available only with ManageWise, not with ZENworks Server Management.

GroupWise MIB Files

The GroupWise MIB files include the standard SNMP management information. In addition, the files include annotations that enhance the Alert functions of ManageWise.

For example, the Summary provides more detailed information than the Description does in other SNMP management programs. The ManageWise annotations are embedded in comments; therefore, they have no affect on other SNMP management programs.

GroupWise Agent Alarm Help File

When GroupWise alarms appear in ManageWise, you can double-click the alarm to display the alarm information contained in the Agent Alarm help file. To enable this feature, copy the gwalarm.hlp file from the \agents\snmp directory to the \mw\nms\help directory on your ManageWise station. This help file explains the alarms each agent might produce by giving a description, cause, and action for each alarm.

Configuring the MTA for SNMP Monitoring

In order for SNMP monitoring programs to monitor the MTA, the MTA must be configured with a network address and SNMP community string.

1. In ConsoleOne, browse to and right-click the MTA object, then click Properties.
2. Click GroupWise > Network Address to display the Network Address page.
3. Click the pencil icon to provide the TCP/IP address or IPX™/SPX™ address of the server where the MTA runs, then click Apply.
4. Click GroupWise > Agent Settings.
5. Provide your system SNMP community GET string, then click OK.

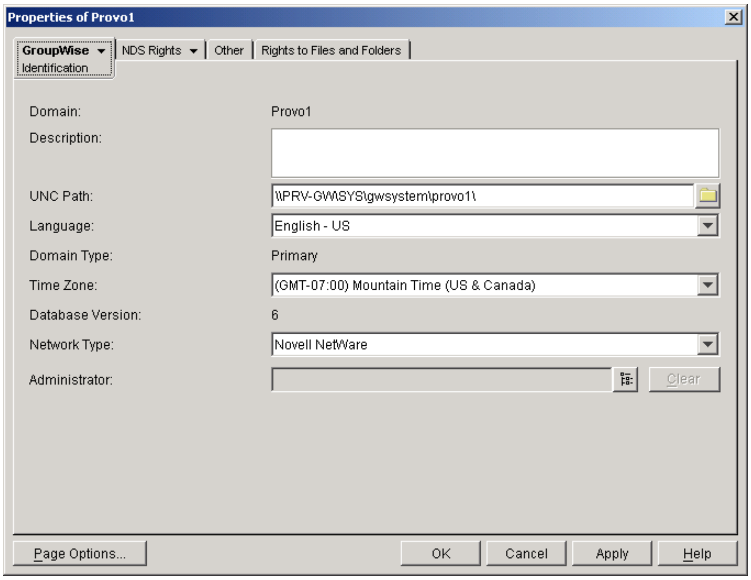
   ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

   The MTA should now be visible to your SNMP monitoring program.

Notifying the Domain Administrator

If you want to be notified with an e-mail message whenever the MTA encounters a critical error, you can designate yourself as an administrator of the domain for which the MTA is running.

1 In ConsoleOne, browse to and right-click the Domain object, then click Properties to display the Identification page.



Domain: Provo1

Description:

UNC Path: \\PRV-GW\SYS\gwsystem\provo1\

Language: English - US

Domain Type: Primary

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Database Version: 6

Network Type: Novell NetWare

Administrator:

2 In the Administrator field, browse to and select your GroupWise user ID.

A domain can have a single administrator, or you can create a group to function as administrators.

3 Click OK to save the administrator information.

The selected user or group will then begin receiving e-mail messages whenever the MTA for the domain encounters a critical error.

Corresponding Startup Switches

By default, the MTA will generate error mail if an administrator has been assigned for the domain. Error mail can be turned off using the /noerrormail switch.

POA Web Console

Another way to receive e-mail notification of POA problems is to use GroupWise Monitor to access the POA Web console. See "Configuring E-Mail Notification" on page 918.

Using the MTA Error Message Documentation

MTA error messages are documented with the source and explanation of the error, possible causes of the error, and actions to take to resolve the error. See "Message Transfer Agent Error Messages" in *GroupWise 6.5 Troubleshooting 1: Error Messages*.

Employing MTA Troubleshooting Techniques

If you are having a problem with the MTA but not receiving a specific error message, or if the suggested actions for the specific error did not resolve the problem, you can review more general troubleshooting strategies for dealing with MTA problems. See "Message Transfer Agent Problems" in "Strategies for Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

You can also use GroupWise Monitor to troubleshoot message transfer problems. See "Monitor" on page 901.

Using Platform-Specific MTA Monitoring Tools

Each operating system where the MTA runs provides tools for monitoring programs.

- "NetWare Monitoring Tools" on page 633
- "Linux Monitoring Tools" on page 633
- "Windows Monitoring Tools" on page 633

NetWare Monitoring Tools

If you are running the MTA on NetWare servers, you can use the NetWare Monitor NLM to monitor the effects of the MTA on the NetWare server. NetWare 6.*x* provides monitoring tools that you can use from your Web browser. Processor, resource, and memory utilization can be compared to other non-GroupWise NLM programs to determine if the MTA NLM program is monopolizing resources. See your NetWare documentation for additional monitoring suggestions.

Linux Monitoring Tools

If you are running the MTA on Linux servers, you can use SNMP tools like snmpget and snmpwalk that allow you to retrieve the data about all the services registered with the SNMP service. These tools are part of the NET-SNMP package. See your Linux documentation for additional monitoring suggestions.

Windows Monitoring Tools

If you are running the MTA on Windows servers, you can use the Performance Monitor in Windows Administrator Tools to gather similar information. See your Windows documentation for additional monitoring suggestions.

Using MTA Message Logging

For extremely detailed monitoring of message flow, you can configure the MTA to gather a variety of statistics. See "Enabling MTA Message Logging" on page 603.

45 Optimizing the MTA

You can adjust how the MTA functions to optimize its performance. Before attempting optimization, you should run the MTA long enough to observe its efficiency and its impact on other network applications running on the same server. See Chapter 44, “Monitoring the MTA,” on page 605.

Also, remember that optimizing your network hardware and operating system can make a difference in MTA performance.

The following topics help you optimize the MTA:

- “Optimizing TCP/IP Links” on page 635
- “Optimizing Mapped/UNC Links” on page 636
- “Optimizing the Routing Queue” on page 639
- “Adjusting MTA Polling of Closed Locations” on page 640

Optimizing TCP/IP Links

Using startup switches in the MTA startup file, you can fine-tune the performance of TCP/IP links.

- “Adjusting the Number of MTA TCP/IP Connections” on page 635
- “Adjusting the MTA Wait Intervals for Slow TCP/IP Connections” on page 636

Adjusting the Number of MTA TCP/IP Connections

When using TCP/IP links between domains, you can control the number of inbound connections the MTA can establish for receiving messages.

Use the /tcpinbound switch in the MTA startup file to increase the maximum number of inbound connections the MTA can establish from the default of 40 to whatever setting meets the needs of your system. There is no maximum setting.

If the MTA is receiving more requests than it can accept, the sending MTAs must wait until a connection becomes available, which slows down message transfer. Each connection requires only about 20 KB. For example, if you configure the MTA to accept 600 connections, it would require approximately 12 MB of RAM. Although there is no maximum setting for inbound connections, this setting is adequate to handle very heavy usage. Use lower settings to conserve RAM or for lighter usage.

MTA Web Console
You can check the maximum number of TCP/IP connections that the MTA can start on the Configuration page under the TCP/IP Settings heading.

Adjusting the MTA Wait Intervals for Slow TCP/IP Connections

When using TCP/IP links, you can control how long the MTA waits for responses.

By default, the MTA waits 5 seconds for a response when trying to contact another MTA or a POA across a TCP/IP link. If no response is received from the other MTA or the POA, the sending MTA tries again three more times. If all four attempts fail, the MTA reports an error, then waits 10 minutes before it tries again.

When the MTA attempts to send messages to another MTA or a POA across a TCP/IP link, the sending MTA tries for 20 seconds before reporting an error.

On some networks, these wait intervals might not be sufficient, and the MTA might report an error when, by waiting longer, the needed connection or data transfer would be able to take place.

Use the /tcpwaitconnect switch in the MTA startup file to increase the number of seconds the MTA waits for a response from another MTA or a POA across a TCP/IP link.

Use the /tcpwaitdata switch in the MTA startup file to increase the number of seconds the MTA attempts to send messages to another MTA or a POA across a TCP/IP link.

MTA Web Console
You can check the current wait intervals on the Configuration page under the TCP/IP Settings heading.

Optimizing Mapped/UNC Links

If you must use mapped or UNC links, you can fine-tune how the MTA polls its input queues.

- "Using TCP/IP Links between Locations" on page 636
- "Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways" on page 636
- "Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices" on page 638

NOTE: The Linux MTA does not use mapped or UNC links.

Using TCP/IP Links between Locations

TCP/IP links between domains or between a domain and its post offices are faster than mapped or UNC links because the MTA is immediately notified whenever a new message arrives. This eliminates the latency involved in scanning input directories for messages to process. To change from mapped or UNC links to TCP/IP links, see "Using TCP/IP Links between Domains" on page 579 and "Using TCP/IP Links between a Domain and its Post Offices" on page 583

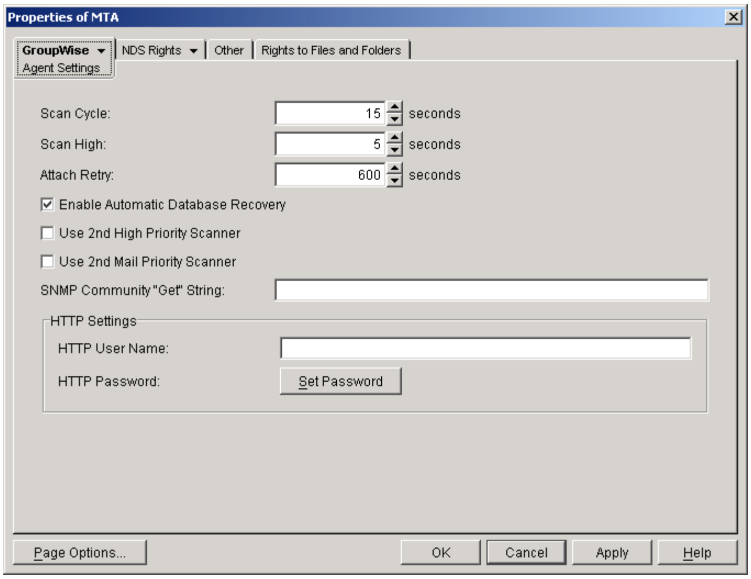
Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways

When using mapped or UNC links between the local domain and its post offices and other domains, the MTA can create a lot of network traffic just scanning its input queues, especially if the message load is light. This can be minimized by setting the scan cycle to a higher number. On the other hand, if the scan cycle is set too high, important messages might have to wait in the input queues to be picked up by the MTA. The MTA's scan cycle settings also control how often it communicates with gateways installed in the domain.

By default, when using mapped or UNC links, the MTA scans its high priority queues every 5 seconds and its regular and low priority queues every 15 seconds. You can adjust the scan cycle settings to meet the needs of your GroupWise® system.

1 In ConsoleOne®, browse to and right-click the MTA object, then click Properties.

2 Click GroupWise > Agent Settings to display the Agent Settings page.



Scan Cycle: 15 seconds

Scan High: 5 seconds

Attach Retry: 600 seconds

☑ Enable Automatic Database Recovery

☐ Use 2nd High Priority Scanner

☐ Use 2nd Mail Priority Scanner

SNMP Community "Get" String:

HTTP Settings

HTTP User Name:

HTTP Password: Set Password

3 Decrease the number of seconds in the Scan Cycle field if you want the MTA to scan the regular and low priority queues (2-7) more often.

or

Increase the number of seconds in Scan Cycle field if you want the MTA to scan the regular and low priority queues (2-7) less often.

4 Decrease the number of seconds in the Scan High field if you want the MTA to scan the high priority queues (0-1) more often.

or

Increase the number of seconds in the Scan High field if you want the MTA to scan high priority queues (0-1) less often.

For the locations and specific uses of the MTA input queues, see "Message Transfer/Storage Directories" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

5 Click OK to save the new scan cycle settings.

ConsoleOne then notifies the MTA to restart so the new settings can be put into effect.

Corresponding Startup Switches

You could also use the /cylo and /cyhi switches in the MTA startup file to adjust the MTA scan cycle.

MTA Web Console

You can check the current MTA scan cycle on the Configuration page under the Performance Settings heading.

Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices

When using mapped or UNC links, the MTA automatically starts one high priority scanner thread for the priority 0 and 1 subdirectories of its input queues. It also starts a second scanner thread for the priority 2-7 subdirectories. This default configuration can create a bottleneck under some circumstances:

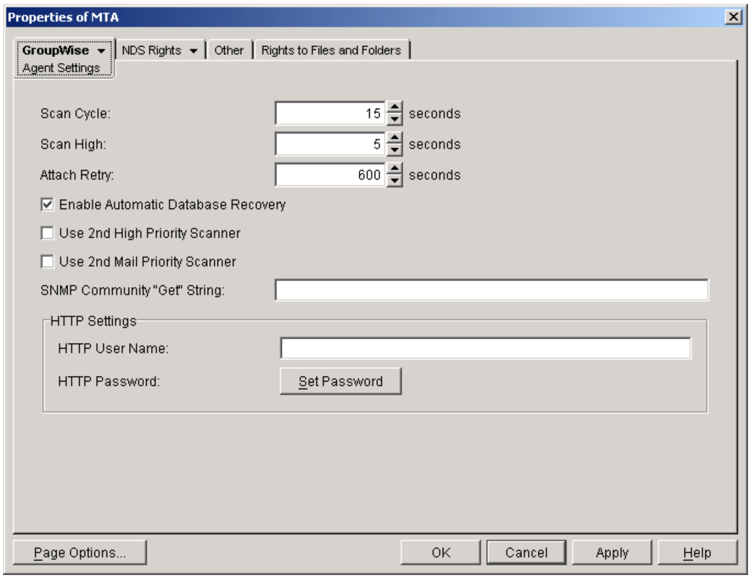
- The priority 0 subdirectory is used for Busy Search requests from GroupWise client users. The priority 1 subdirectory is used by GroupWise Remote users. If your GroupWise system serves a large number of very active GroupWise Remote users, the MTA can stay busy processing requests from Remote users, causing other users to experience a delay in response to a Busy Search request.
- The priority 2 subdirectory is used for administrative messages and high priority user messages. Priority 3-7 subdirectories are used for regular and low priority messages and status messages. Certain administrative activities, such as moving a large number of users or purging trash, can create numerous administrative messages in the priority 2 subdirectory, causing users to experience a delay in receiving high priority as well as regular messages.

For the locations of the MTA input queues, see "Message Transfer/Storage Directories" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

You can configure the MTA so that it starts separate scanner threads to service the priority 1 and 2 subdirectories and/or separate scanner threads for the 2-3 and 4-7 subdirectories.

IMPORTANT: Do not try to run more than one MTA for the same domain.

1. In ConsoleOne, browse to and right-click the MTA object, then click Properties.
2. Click GroupWise > Agent Settings to display the Agent Settings page.



Scan Cycle: 15 seconds

Scan High: 5 seconds

Attach Retry: 600 seconds

☑ Enable Automatic Database Recovery

□ Use 2nd High Priority Scanner

□ Use 2nd Mail Priority Scanner

SNMP Community "Get" String:

HTTP Settings

HTTP User Name:

HTTP Password: Set Password

3. Select Use 2nd High Priority Scanner to provide separate MTA scanner threads for Busy Searches and GroupWise Remote users.
4. Select Use 2nd Mail Priority Scanner to provide separate MTA scanner threads for administrative messages and high priority user messages vs. regular and low priority messages.

These settings can be used separately (creating three MTA scanner threads) or together (creating four MTA scanner threads).

Primary Use	Priority Directory	Default Operation	2nd High Priority Scanner	2nd Mail Priority Scanner	Both Second Priority Scanners
Busy searches	wpcsin\0	High priority scanner thread	High priority scanner thread one	High priority scanner thread	High priority scanner thread one
GroupWise Remote user requests	wpcsin\1		High priority scanner thread two		High priority scanner thread two
Administrative requests and high priority messages	wpcsin\2	Mail priority scanner thread	Mail priority scanner thread	Mail priority scanner thread one	Mail priority scanner thread one
High priority statuses	wpcsin\3				
Normal priority messages	wpcsin\4			Mail priority scanner thread two	Mail priority scanner thread two
Normal priority statuses	wpcsin\5				
Low priority messages	wpcsin\6				
Low priority statuses	wpcsin\7				
Total Scanner Threads in Use:		2	3	3	4

5 Click OK to save the new scanner thread settings.

ConsoleOne then notifies the MTA to restart so the new setting can be put into effect.

Corresponding Startup Switches

You could also use the /fast0 and /fast4 switches in the MTA startup file to adjust the allocation of MTA scanner threads.

MTA Web Console

You can check the current MTA scan cycle on the Configuration page under the Performance Settings heading.

Optimizing the Routing Queue

Using startup switches in the MTA startup file, you can fine-turn MTA processing in of the routing queue. When the MTA starts, it starts one or more router threads to process its routing queue (gwinprog). As messages arrive in the routing queue, it starts additional routers as needed, within parameters you can set.

- "Adjusting the Maximum Number of Active Router Threads" on page 640
- "Adjusting the Maximum Number of Idle Router Threads" on page 640

MTA Web Console
You can view the current contents of the routing queue from the Configuration page. Click Router under the Queue Information heading.

Adjusting the Maximum Number of Active Router Threads

By default, the MTA will continue to start additional router threads to processes messages in the routing queue as long as message traffic demands it, until as many as 16 router threads are running. Use the /maxrouters switch in the MTA startup file to control the number of router threads the MTA can start.

Set /maxrouters to a lower number to conserve resources and keep the MTA from starting more than the specified maximum number of router threads.

Adjusting the Maximum Number of Idle Router Threads

By default, after the MTA starts a router thread, it keeps it running, up to the maximum number specified by the /maxrouters switch. In a system where short bursts of heavy message traffic are followed by extended lulls, idle router threads could be consuming resources that would be better used by other processes. Use the /maxidlerouters switch in the MTA startup file to determine how many idle router threads are allowed to remain running. The default is 16 idle router threads.

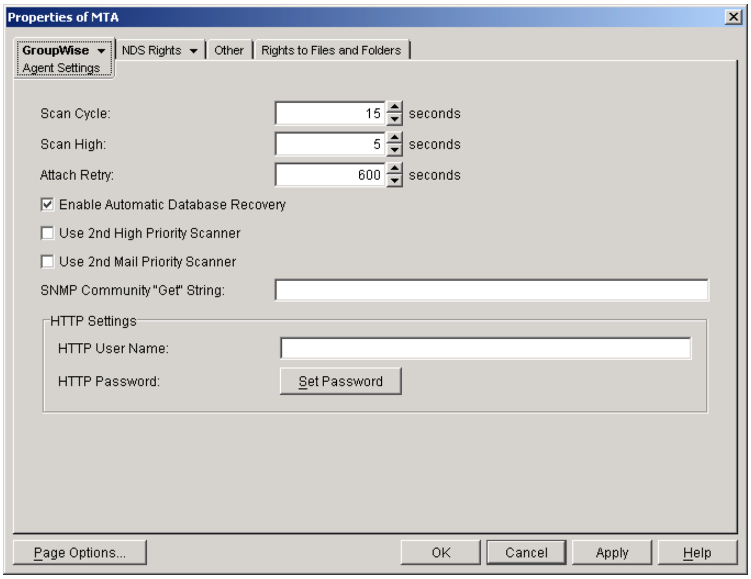
Set /maxidlerouters to a lower number if you want the MTA to terminate idle router threads more quickly. Set /maxidlerouters to a higher number if you want the MTA to keep more idle router threads ready to process incoming message traffic.

Adjusting MTA Polling of Closed Locations

When a location becomes closed (unavailable), the MTA waits before attempting to recontact that location. If the MTA waits only a short period of time, the MTA can waste time and create network traffic by trying to reestablish a connection with a closed location. On the other hand, you do not want the MTA to ignore an available location by waiting too long.

By default, the MTA waits 600 seconds (10 minutes) between its attempts to contact a closed location. You can adjust the time interval the MTA waits to meet the needs of your GroupWise system.

1. In ConsoleOne, browse to and right-click the MTA object, then click Properties.
2. Click GroupWise > Agent Settings to display the Agent Settings page.



Scan Cycle: 15 seconds

Scan High: 5 seconds

Attach Retry: 600 seconds

☑ Enable Automatic Database Recovery

□ Use 2nd High Priority Scanner

□ Use 2nd Mail Priority Scanner

SNMP Community "Get" String:

HTTP Settings

HTTP User Name:

HTTP Password: Set Password

3 Decrease the number of seconds in the Attach Retry field if you want the MTA to try to contact closed locations more often.

or

Increase the number of seconds in Attach Retry field if you want the MTA to try to contact closed locations less often.

4 Click OK to save the new Attach Retry setting.

ConsoleOne then notifies the MTA to restart so the new setting can be put into effect.

For a TCP/IP link, a location is considered open if the MTA receives a response from the receiving agent within the currently configured wait intervals. See "Adjusting the MTA Wait Intervals for Slow TCP/IP Connections" on page 636. Otherwise, the location is considered closed.

For a mapped or UNC link, a location is considered open if the MTA can perform the following actions:

- Create a temporary directory in the MTA input queue (*domain*\wpcsin and *post_office*\wpcsin directories)
- Create a temporary file in that new directory
- Delete the temporary file
- Delete the temporary directory

For more information about the MTA input queues, see "Message Transfer/Storage Directories" in *GroupWise 6.5 Troubleshooting 3: Message Flow and Directory Structure*.

46 Using MTA Startup Switches

You can override settings provided in ConsoleOne® by using startup switches. You can override startup switches provided in the startup file by using startup switches on the command line. For more information about starting the MTA, see "Starting the MTA" on page 568.

The table below summarizes MTA startup switches for all platforms and how they correspond to configuration settings in ConsoleOne.

NetWare MTA	Linux MTA	Windows MTA	ConsoleOne Settings
@filename	*@filename*	*@filename*	N/A
N/A	--activelog	/activelog	N/A
/certfile	--certfile	/certfile	Certificate File
/cyhi	--cyhi	/cyhi	Scan High
/cylo	--cylo	/cylo	Scan Cycle
/defaultroutingdomain	--defaultroutingdomain	/defaultroutingdomain	Default Routing Domain
/dn	N/A	N/A	N/A
/fast0	--fast0	/fast0	Use 2nd High Priority Scanner
/fast4	--fast4	/fast4	Use 2nd Mail Priority Scanner
/help	--help	/help	N/A
/home	--home	/home	N/A
/httppassword	--httppassword	/httppassword	HTTP Password
/httpport	--httpport	/httpport	HTTP Port
/httprefresh	--httprefresh	/httprefresh	N/A
/httpssl	--httpssl	/httpssl	HTTP
/httpuser	--httpuser	/httpuser	HTTP User Name
/keyfile	--keyfile	/keyfile	SSL Key File
/keypassword	--keypassword	/keypassword	SSL Key File Password
/language	--language	/language	N/A
/liveremote	--liveremote	/liveremote	N/A

NetWare MTA	Linux MTA	Windows MTA	ConsoleOne Settings
/log	--log	/log	Log File Path
/logdays	--logdays	/logdays	Max Log File Age
/logdiskoff	--logdiskoff	/logdiskoff	Logging Level
/loglevel	--loglevel	/loglevel	Logging Level
/logmax	--logmax	/logmax	Max Log Disk Space
/lrconn	--lrconn	/lrconn	N/A
/lrwaitdata	--lrwaitdata	/lrwaitdata	N/A
/maxidlerouters	--maxidlerouters	/maxidlerouters	N/A
/maxrouters	--maxrouters	/maxrouters	N/A
/messagelogdays	--messagelogdays	/messagelogdays	Delete Reports After
/messagelogmaxsize	--messagelogmaxsize	/messagelogmaxsize	N/A
/messagelogpath	--messagelogpath	/messagelogpath	Message Log File Path
/messagelogsettings	--messagelogsettings	/messagelogsettings	Message Logging Level
/msgtranssl	--msgtranssl	/msgtranssl	Message Transfer SSL
/noada	--noada	/noada	N/A
/nodns	--nodns	/nodns	N/A
/noerrormail	--noerrormail	/noerrormail	N/A
/nondssync	--nondssync	/nondssync	N/A
/norecover	--norecover	/norecover	N/A
/nosnmp	--nosnmp	/nosnmp	N/A
/password	N/A	N/A	N/A
/tcpinbound	--tcpinbound	/tcpinbound	N/A
/tcpport	--tcpport	/tcpport	Network Address
/tcpwaitconnect	--tcpwaitconnect	/tcpwaitconnect	N/A
/tcpwaitdata	--tcpwaitdata	/tcpwaitdata	N/A
/tracelogin	N/A	N/A	N/A
/user	N/A	N/A	N/A
/work	--work	/work	N/A

@filename

Specifies the location of the MTA startup file. On NetWare and Windows, the full path must be included if the file does not reside in the same directory with the MTA program. On Linux, the startup file always resides in the /opt/novell/groupwise/agents/share directory. The startup file must reside on the same server where the MTA is installed. For more information about the MTA startup file, see "Starting the MTA" on page 568.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	@[*vol*:][*dir*\]*file*@\\*svr**vol**dir**file*	@[/*dir*/]*file*	@[*drive*:][*dir*\]*file* @\\*svr**sharename**dir**file*
Example:	load gwmta @provo2.mta load gwmta @sys:\agt\provo2.mta load gwmta @\\s2\sys\agt\provo2.mta	./gwmta @../share/lnxdom.mta	gwmta.exe @provo2.mta gwmta.exe @d:\agt\provo2.mta gwmta.exe @\\s2\c\agt\provo2.mta

/activelog

Displays the active log window rather than the alert box when the MTA starts. See "Monitoring the MTA from the MTA Agent Console" on page 605.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	N/A	--activelog	/activelog

/certfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the MTA and other programs. See "Enhancing Domain Security with SSL Connections to the MTA" on page 589.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/certfile-[*svr*\][*vol*:]*dir**file* /certfile-\\*svr**vol**dir**file*	--certfile-/*dir*/*file*	/certfile-[*drive*:]*dir**file* /certfile-\\*svr**sharename**dir**file*
Example:	/certfile-\ssl\gw.crt /certfile-server2\sys:\ssl\gw.crt /certfile-\\server2\sys\ssl\gw.crt	--certfile /certs/gw.crt	/certfile-\ssl\gw.crt /certfile-m:\ssl\gw.crt /certfile-\\server2\c\ssl\gw.crt

See also /keyfile and /keypassword.

/cyhi

Sets the number of seconds in the scan cycle that the MTA uses to scan its priority 0-1 input queues. The default is 5 seconds. See "Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways" on page 636.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/cyhi-*seconds*	--cyhi-*seconds*	/cyhi-*seconds*
Example:	/cyhi-3	--cyhi 3	/cyhi-3

See also /cylo.

/cylo

Sets the number of seconds in the scan cycle that the MTA uses to scan its priority 2-7 input queues. The default is 15 seconds. See "Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways" on page 636.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/cylo-*seconds*	--cylo-*seconds*	/cylo-*seconds*
Example:	/cylo-10	--cylo 10	/cylo-10

See also /cyhi.

/defaultroutingdomain

Identifies the domain name in your GroupWise® system to which all MTAs should send messages when they cannot resolve the available routing information to a specific *user.post_office.domain* GroupWise address. See "Using Routing Domains" on page 591.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/defaultroutingdomain-*domain*	--defaultroutingdomain *domain*	/defaultroutingdomain-*domain*
Example:	/defaultroutingdomain-inethub	--defaultroutingdomain inethub	/defaultroutingdomain-inethub

/dn

Specifies the Novell® eDirectory™ distinguished name of the NetWare® MTA object to facilitate logging into remote servers and authenticating to eDirectory. It can be used instead of the /user and /password switches.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/dn-*distinguished_name*	N/A	N/A
Example:	/dn-MTA.provo2.GroupWise	N/A	N/A

/fast0

Causes the MTA to monitor and process the priority 0 and 1 subdirectories independently with separate scanner threads, rather than in sequence with the same scanner thread. See "Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices" on page 638.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/fast0	--fast0	/fast0

See also /fast4.

/fast4

Causes the MTA to monitor and process the priority 2 and 3 subdirectories with a separate scanner thread from the priority 4 through 7 subdirectories. See "Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices" on page 638.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/fast4	--fast4	/fast4

See also /fast0.

/help

Displays the MTA startup switch Help information. When this switch is used, the MTA does not start.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/help or /?	--help or --?	/help or /?
Example:	load gwmta.nlm /help	./gwmta.exe --help	gwmta.exe /help

/home

Specifies the domain directory, where the MTA can access the domain database (wpdomain.db). There is no default location. You must use this switch in order to start the MTA. See "Starting the MTA" on page 568.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/home-[*svr*\][*vol*:]*\dir* /home-\\svr\vol\dir	--home /*dir*	/home-[*drive*:]*\dir* /home-\\svr\sharename\dir
Example:	/home-\provo2 /home-mail:\provo2 /home-server2\mail:\provo2 /home-\\server2\mail\provo2	--home /gwsystem/provo2	/home-\provo2 /home-m:\provo2 /home-\\server2\c\mail\provo2

/httppassword

Specifies the password for the MTA to prompt for before allowing MTA status information to be displayed in your Web browser. Do not use an existing eDirectory password because the information passes over the insecure connection between your Web browser and the MTA. See "Using the MTA Web Console" on page 617.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/httppassword-*unique_password*	--httppassword *unique_password*	/httppassword-*unique_password*
Example:	/httppassword-AgentWatch	--httppassword AgentWatch	/httppassword-AgentWatch

See also /httpuser, /httpport, /httprefresh, and /httpssl.

/httpport

Sets the HTTP port number used for the MTA to communicate with your Web browser. The default is 7180; the setting must be unique. See "Using the MTA Web Console" on page 617.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/httpport-*port_number*	--httpport *port_number*	/httpport-*port_number*
Example:	/httpport-3801	--httpport 3802	/httpport-3803

See also /httpuser, /httppassword, /httprefresh, and /httpssl.

/httprefresh

Specifies the rate at which the MTA refreshes the status information in your Web browser. The default is 60 seconds. See "Using the MTA Web Console" on page 617.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/httprefresh-*seconds*	--httprefresh *seconds*	/httprefresh-*seconds*
Example:	/httprefresh-30	--httprefresh 90	/httprefresh-120

See also /httpuser, /httppassword, /httpport, and /httpssl.

/httpssl

Enables secure SSL communication between the MTA and the MTA Web console displayed in your Web browser. See "Enhancing Domain Security with SSL Connections to the MTA" on page 589.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/httpssl	--httpssl	/httpssl

See also /certfile, /keyfile, and/keypassword.

/httpuser

Specifies the username for the MTA to prompt for before allowing MTA status information to be displayed in your Web browser. Providing a username is optional. Do not use an existing eDirectory username because the information passes over the insecure connection between your Web browser and the MTA. See "Using the MTA Web Console" on page 617.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/httpuser-*unique_name*	--httpuser *unique_name*	/httpuser-*unique_name*
Example:	/httpuser-GWWebCon	--httpuser GWWebCon	/httpuser-GWWebCon

See also /httppassword, /httpport, and /httprefresh.

/keyfile

Specifies the full path to the private file used to provide secure SSL communication between the MTA and other programs. See "Enhancing Domain Security with SSL Connections to the MTA" on page 589.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/keyfile-[*svr*\][*vol*:]*dir**file* /keyfile-\\*svr**vol**dir**file*	--keyfile /*dir*/*file*	/keyfile-[*drive*:]*dir**file* /keyfile-\\*svr**sharename**dir**file*
Example:	/keyfile-\ssl\gw.key /keyfile-server2\sys:\ssl\gw.key /keyfile-\\server2\sys\ssl\gw.key	--keyfile /ssl/gw.key	/keyfile-\ssl\gw.key /keyfile-m:\ssl\gw.key /keyfile-\\server2\c\ssl\gw.key

See also /certfile and /keypassword.

/keypassword

Specifies the password used to encrypt the private SSL key file when it was created. See "Enhancing Domain Security with SSL Connections to the MTA" on page 589.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/keypassword-*password*	--keypassword *password*	/keypassword-*password*
Example:	/keypassword-gwssl	--keypassword gwssl	/keypassword-gwssl

See also /certfile and /keyfile.

/language

Specifies the language to run the MTA in, using a two-letter language code as listed below. You must install the MTA in the selected language in order for the MTA to display in the selected language.

The initial default is the language used in the domain. If that language has not been installed, the next default is the language used by the operating system. If that language has not been installed, the final default is English. You only need to use this switch if you need to override these defaults.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/language-*code*	--language *code*	/language-*code*
Example:	/language-es	--language de	/language-fr

The table below lists the valid language codes. Contact your local Novell sales office for information about language availability.

Language	Language Code	Language	Language Code
Arabic	AR	Hungarian	MA
Czechoslovakian	CS	Italian	IT
Chinese-Simplified	CS	Japanese	NI
Chinese-Traditional	CT	Korean	KR
Danish	DK	Norwegian	NO
Dutch	NL	Polish	PL
English-United States	US	Portuguese-Brazil	BR
Finnish	SU	Russian	RU
French-France	FR	Spanish	ES
German-Germany	DE	Swedish	SV
Hebrew	HE	Turkish	TR

/liveremote

Turns on re-direction of Remote client requests and provides the TCP port on which the MTA listens for Remote client requests. See "Enabling Live Remote" on page 589.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/liveremote-*port_number*	/liveremote-*port_number*	/liveremote-*port_number*
Example:	/liveremote-7111	/liveremote-7112	/liveremote-7112

See also /lrconn and /lrwaitdata.

/log

Specifies the directory where the MTA will store its log files. On NetWare and Windows, the default location is the mslocal directory in the directory specified by the /work switch. On Linux, the default location is the /var/log/novell/groupwise/*domain_name*.mta directory. See "Using MTA Log Files" on page 625.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/log-[*svr*\][*vol*:]*dir* /log-\\*svr**vol**dir*	--log /*dir*	/log-[*drive*:]*dir* /log-\\*svr**sharename**dir*
Example:	/log-\agt\log /log-server2\mail:\agt\log /log-\\server2\mail\agt\log	--log /gwsystem/logs	/log-\agt\log /log-m:\agt\log /log-\\server2\c\mail\agt\log

Typically you would find multiple log files in the specified directory. The first 4 characters represent the date. The next 3 characters identify the agent. A three-digit extension allows for multiple log files created on the same day. For example, a log file named 0518mta.001 would indicate that it is an MTA log file, created on May 18. If you restarted the MTA on the same day, a new log file would be started, named 0518mta.002.

See also /loglevel, /logdiskoff, /logdays, and /logmax.

/logdays

Sets the number of days you want MTA log files to remain on disk before being automatically deleted. The default log file age is 7 days. See "Using MTA Log Files" on page 625.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/logdays-*days*	--logdays *days*	/logdays-*days*
Example:	/logdays-5	--logdays 10	/logdays-14

See also /log, /loglevel, /logdiskoff, and /logmax.

/logdiskoff

Turns off disk logging for the MTA so no information about the functioning of the MTA is stored on disk. The default is for logging to be turned on. See "Using MTA Log Files" on page 625.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/logdiskoff	--logdiskoff	/logdiskoff

See also /loglevel.

/loglevel

Controls the amount of information logged by the MTA. Logged information is displayed in the log message box and written to the MTA log file during the current agent session. The default is Normal, which displays only the essential information suitable for a smoothly running MTA. Use Verbose to display the essential information, plus additional information helpful for troubleshooting. Verbose logging does not degrade MTA performance, but log files saved to disk consume more disk space when verbose logging is in use. See "Using MTA Log Files" on page 625.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/loglevel-*level*	--loglevel *level*	/loglevel-*level*
Example:	/loglevel-verbose	--loglevel verbose	/loglevel-verbose

See also /log, /logdiskoff, /logdays, and /logmax.

/logmax

Sets the maximum amount of disk space for all MTA log files. When the specified disk space is consumed, the MTA deletes existing log files, starting with the oldest. The default is 65536 KB of disk space for all MTA log files. See "Using MTA Log Files" on page 625.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/logmax-*kilobytes*	--logmax *kilobytes*	/logmax-*kilobytes*
Example:	/logmax-32000	--logmax 130000	/logmax-160000

See also /log, /loglevel, /logdiskoff, and /logdays.

/lrconn

Specifies the maximum number of simultaneously connected Remote client users the MTA can accept. The default is 25. See "Enabling Live Remote" on page 589.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/lrconn-*number*	--lrconn *number*	/lrconn-*number*
Example:	/lrconn-50	--lrconn 75	/lrconn-100

See also /liveremote and /lrwaitdata.

/lrwaitdata

Specifies the number of seconds you want the MTA to wait for a response from the PO before timing out for users in Remote mode. The default is 5 minutes. See "Enabling Live Remote" on page 589.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/lrwaitdata-*number*	--lrwaitdata *number*	/lrwaitdata-*number*
Example:	/lrwaitdata-7	--lrwaitdata-10	/lrwaitdata-12

See also /liveremote and /lrconn.

/maxidlerouters

Specifies the maximum number of idle router threads the MTA can keep running. The default is 16; valid values range from 1 to 16. See "Optimizing the Routing Queue" on page 639.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/maxidlerouters-*threads*	--maxidlerouters *threads*	/maxidlerouters-*threads*
Example:	/maxidlerouters-5	--maxidlerouters 10	/maxidlerouters-12

See also /maxrouters.

/maxrouters

Specifies the maximum number of router threads the MTA can start. The default is 16; valid values range from 1 to 16. See "Optimizing the Routing Queue" on page 639.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/maxrouters-*threads*	--maxrouters *threads*	/maxrouters-*threads*
Example:	/maxrouters-10	--maxrouters 12	/maxrouters-14

See also /maxidlerouters.

/messagelogdays

Sets the number of days you want MTA message log files to remain on disk before being automatically deleted. The default is 7 days. See "Enabling MTA Message Logging" on page 603.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/messagelogdays-*days*	--messagelogdays *days*	/messagelogdays-*days*
Example:	/messagelogdays-5	--messagelogdays 10	/messagelogdays-14

See also /messagelogsettings, /messagelogpath, and /messagelogmaxsize.

/messagelogmaxsize

Sets the maximum size for MTA message log files. The default is 65536 KB. See "Enabling MTA Message Logging" on page 603.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/messagelogmaxsize-*kilobytes*	--messagelogmaxsize *kilobytes*	/messagelogmaxsize-*kilobytes*
Example:	/messagelogmaxsize-32000	--messagelogmaxsize 130000	/messagelogmaxsize-160000

See also /messagelogsettings, /messagelogpath, and /messagelogdays.

/messagelogpath

Specifies the directory for the MTA message log. See "Enabling MTA Message Logging" on page 603.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/messagelogpath-[*svr*\][*vol*:]\dir /messagelogpath-\\svr\vol\dir	--messagelogpath /*dir*	/messagelogpath-[*drive*:]\dir /messagelogpath-\\svr\sharename\dir
Example:	/messagelogpath-\mta\log /messagelogpath-svr2\mail:\mta\log /messagelogpath-\\\\svr2\mail\mta\log	--messagelogpath /gwsys/logs	/messagelogpath-\mta\log /messagelogpath-m:\mta\log /messagelogpath-\\\\svr2\c\mail\mta\log

See also /messagelogsettings, /messagelogdays, and /messagelogmaxsize.

/messagelogsettings

Enables MTA message logging. See "Enabling MTA Message Logging" on page 603.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/messagelogsettings-*codes*	--messagelogsettings *codes*	/messagelogsettings-*codes*
Example:	/messagelogsettings-e	--messagelogsettings e	/messagelogsettings-e

One code or any combination of codes can be used.

Code	Description
e	Enabled; all messages are logged by default
v	Verbose logging; all information is logged
r	Log message delivery/non-delivery reports
s	Log message statuses
o	Log other message types, such as administrative messages for database updates
c	Correlate reports with messages

See also /messagelogpath, /messagelogdays, and /messagelogmaxsize.

/msgtranssl

Enables secure SSL communication between the MTA and the POAs in its domain. See "Enhancing Domain Security with SSL Connections to the MTA" on page 589.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/msgtranssl	--msgtranssl	/msgtranssl

See also /certfile, /keyfile, and /keypassword.

/noada

Disables the MTA admin thread. For an explanation of the MTA admin thread, see "MTA Admin Thread Status Box" on page 608.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/noada	--noada	/noada

Historical Note: In GroupWise 5.2 and earlier, a separate agent, the Administration Agent (ADA), handled the functions now consolidated into the MTA admin thread. Hence the switch name, / noada.

/nodns

Disables DNS lookups for the MTA. See "Using Dynamic Internet Links" in "Connecting to GroupWise 5.x and 6.x Systems" in the *GroupWise 6.5 Multi-System Administration Guide*.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/nodns	--nodns	/nodns

/noerrormail

Prevents error files from being sent to the GroupWise administrator. The default is for error mail to be sent to the administrator. See "Notifying the Domain Administrator" on page 632.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/noerrormail	--noerrormail	/noerrormail

/nondssync

Disables eDirectory user synchronization. See "Using eDirectory User Synchronization" on page 598.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/nondssync	--nondssync	N/A

/norecover

Disables automatic database recovery. The default is for automatic database recovery to be turned on. If the MTA detects a problem with the domain database (wpdomain.db) when automatic database recovery has been turned off, the MTA will notify the administrator, but it will not recover the problem database. See Chapter 26, "Maintaining Domain and Post Office Databases," on page 345.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/norecover	--norecover	/norecover

/nosnmp

Disables SNMP for the MTA. The default is to have SNMP enabled. See "Using SNMP Monitoring Programs" on page 627.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/nosnmp	--nosnmp	/nosnmp

/password

Provides the password for the NetWare MTA to use when accessing domains and post offices on remote servers. See "Starting the MTA" on page 568.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/password-*NetWare_password*	N/A	N/A
Example:	/password-GWise	N/A	N/A

See also /user and /dn.

/tcpinbound

Sets the maximum number of inbound TCP/IP connections for the MTA. The default is 40. There is no maximum number of outbound connections. The only limit on the MTA for outbound connections is available resources. See "Adjusting the Number of MTA TCP/IP Connections" on page 635.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/tcpinbound-*number*	--tcpinbound *number*	/tcpinbound-*number*
Example:	/tcpinbound-50	--tcpinbound 60	/tcpinbound-70

/tcpport

Sets the TCP port number on which the MTA listens for incoming messages. The default is 7100. See "Using TCP/IP Links between Domains" on page 579.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/tcpport-*port_number*	--tcpport *port_number*	/tcpport-*port_number*
Example:	/tcpport-7200	--tcpport 7200	/tcpport-7200

/tcpwaitconnect

Sets the maximum number of seconds the MTA waits for a connection to another MTA. The default is 5. See "Adjusting the MTA Wait Intervals for Slow TCP/IP Connections" on page 636.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/tcpwaitconnect-*seconds*	--tcpwaitconnect *seconds*	/tcpwaitconnect-*seconds*
Example:	/tcpwaitconnect-10	--tcpwaitconnect 10	/tcpwaitconnect-10

See also /tcpwaitdata.

/tcpwaitdata

Sets the maximum number of seconds the MTA attempts to send data over a TCP/IP connection to another MTA. The default is 20. See "Adjusting the MTA Wait Intervals for Slow TCP/IP Connections" on page 636.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/tcpwaitdata-*seconds*	--tcpwaitdata *seconds*	/tcpwaitdata-*seconds*
Example:	/tcpwaitdata-30	--tcpwaitdata 30	/tcpwaitdata-30

See also /tcpwaitconnect.

/tracelogin

Displays NetWare MTA login messages on the NetWare® server console to help determine problems the MTA is having when logging in to a remote server.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/tracelogin-*code*	N/A	N/A
Example:	/tracelogin-1	N/A	N/A

Code	Description
1	Display login problems
2	Display all login messages

/user

Provides the NetWare user ID for the NetWare MTA to use when accessing domains and post offices on remote servers. See "Creating a NetWare Account for Agent Access (Optional)" in the *GroupWise 6.5 Installation Guide*.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/user-NetWare_user_ID	N/A	N/A
Example:	/user-GWAgents	N/A	N/A

See also /password and /dn.

/work

Specifies the directory where the MTA creates its local working directory (mslocal). The default is the domain directory. However, if the domain is located on a different server from where the MTA will run, use a local directory so the MTA cannot lose its connection to its mslocal directory.

	NetWare MTA	Linux MTA	Windows MTA
Syntax:	/work-[*svr*\][*vol*:]*dir* /work-\\*svr**vol**dir*	--work /*dir*	/work-[*drive*:]*dir* /work-\\*svr**sharename**dir*
Example:	/work-\gwmta /work-mail:gwmta /work-server2\mail:\gwmta /work-\\server2\mail\gwmta	--work /gwmta	/work-\gwmta /work-m:\gwmta /work-\\server2\c\mail\gwmta

XI Internet Agent

47 Configuring Internet Agent Services

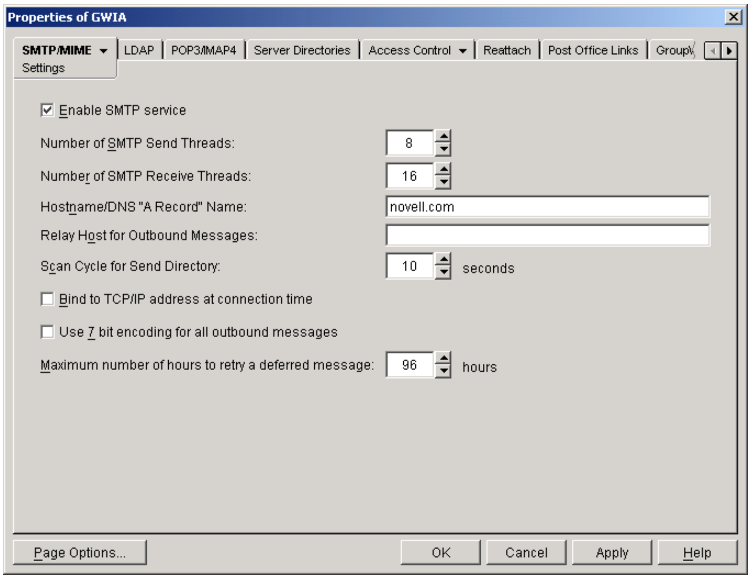
The Internet Agent offers several useful services that you can configure to meet the needs of your GroupWise system.

Configuring SMTP/MIME Services

SMTP and MIME are standard protocols that the GroupWise® Internet Agent uses to send and receive e-mail messages over the Internet. SMTP, or Simple Mail Transfer Protocol, is the message transmission protocol. MIME, or Multipurpose Internet Mail Extension, is the message format protocol. Choose from the following topics for information about how to enable SMTP/MIME services and configure various SMTP/MIME settings:

Configuring Basic SMTP/MIME Settings

1. In ConsoleOne®, right-click the Internet Agent object, then click Properties.
2. If the SMTP/MIME Settings page is not the default page, click SMTP/MIME > Settings.



☑ Enable SMTP service

Number of SMTP Send Threads: 8

Number of SMTP Receive Threads: 16

Hostname/DNS "A Record" Name: novell.com

Relay Host for Outbound Messages:

Scan Cycle for Send Directory: 10 seconds

☐ Bind to TCP/IP address at connection time

☐ Use 7 bit encoding for all outbound messages

Maximum number of hours to retry a deferred message: 96 hours

3 Fill in the fields:

Enable SMTP Service: SMTP service is on by default. This setting allows SMTP Internet messaging. This setting corresponds with the Internet Agent’s /smtp switch.

Number of SMTP Send Threads: The SMTP send threads setting lets you specify the number of threads that will process SMTP send requests. The default is 8 threads. This setting corresponds with the Internet Agent’s /sd switch.

Number of SMTP Receive Threads: The SMTP receive threads setting lets you specify the number of threads that will process SMTP receive requests. The default is 16 threads. This setting corresponds with the Internet Agent’s /rd switch.

Hostname/DNS "A Record" Name: The Hostname/DNS "A Record" name setting lets you identify the hostname of the server where the Internet Agent resides, or in other words the A Record in your DNS table that associates a hostname with the server’s IP address (for example, gwia.novell.com). This setting corresponds with the Internet Agent’s /hn switch.

If the Reject Mail if Sender’s Identity Cannot be Verified setting is turned on (SMTP/MIME tab > Security Settings page), you are required to fill in the Hostname/DNS A Record Name setting. When a TCP/IP communication begins, the two servers involved exchange greetings. Part of the greeting is the recipient server identifying itself. The other part of the greeting is the sending server identifying itself with the SMTP HELO command. The Internet Agent verifies the authenticity of the greetings. If the greeting string does not match the actual Hostname/DNS A Record, the Internet Agent will either pass a warning and continue the communication or terminate the connection.

If you leave this field blank, the Internet Agent uses the fully qualified hostname obtained from your Internet service provider (such as gwia.novell.com), which you should have entered in the Foreign ID field on the Identification page (GroupWise tab).

Relay Host for Outbound Messages: The Relay host setting can be used if you want to use a relay host to route all outbound Internet e-mail. Enter the IP address or DNS hostname of the relay host. The relay host can be part of your network or can reside at the Internet service provider’s site. This setting corresponds with the Internet Agent’s /mh switch.

If you want to use a relay host, but you want some outbound messages sent directly to the destination host rather than to the relay host, you can use a route configuration file (route.cfg). Whenever a message is addressed to a user at a host that is included in the route.cfg file, the

Internet Agent sends the message directly to the host rather than to the relay host. For information about creating a route.cfg file, see "Using a Route Configuration File" on page 676.

Scan Cycle for Send Directory: The Scan cycle setting specifies how often the Internet Agent polls for outgoing messages. The default is 10 seconds. This setting corresponds with the Internet Agent's /p switch.

Bind to TCP/IP Address at Connection Time: Select this option if you want the Internet Agent to bind to the TCP/IP address that has been defined as the Internet Agent's network address (GroupWise tab > Network Address page). When this occurs, the Internet Agent will only use this TCP/IP address when sending outbound messages. This applies to outbound messages only; for inbound messages, it will still listen on all IP addresses assigned to the Internet Agent's server.

This option is useful if the Internet Agent's server has multiple IP addresses and you want to force it to always use the same IP address when sending messages. It is also useful if the Internet Agent is running in a clustered environment (through the use of Novell® Cluster Services™ or Microsoft* Clustering Services) and you want to bind the Internet Agent to the server's secondary IP address.

Use 7 Bit Encoding for All Outbound Messages: By default, the Internet Agent uses 8-bit MIME encoding for any outbound messages that are HTML-formatted or that contain 8-bit characters. If, after connecting with the receiving SMTP host, the Internet Agent discovers that the receiving SMTP host cannot handle 8-bit MIME encoded messages, the Internet Agent converts the messages to 7-bit encoding.

With this option selected, the Internet Agent will automatically use 7-bit encoding and not attempt to use 8-bit MIME encoding. You should use this option if you are using a relay host that does not support 8-bit MIME encoding. This setting corresponds with the Internet Agent's /force7bitout switch.

Maximum Number of Hours to Retry a Deferred Message: Specify the number of hours after which the Internet Agent will stop trying to send deferred messages. The default is 96 hours, or four days. A deferred message is any message that couldn't be sent because of a temporary problem (host down, MX record not found, and so forth).

For the first hour of the specified time, the Internet Agent will try resending the message every 20 minutes. After the first hour, it will try resending the message every four hours. For example, if you specify 10 hours, the Internet Agent will try resending the message at 20 minutes, 40 minutes, 1 hour, 5 hours, and 9 hours. After the 10 hours has expired, it will return an undeliverable status to the sender. This setting corresponds with the Internet Agent's /maxdeferhours switch.

4 Click OK to save the changes.

Using Extended SMTP (ESMTP) Options

The Internet Agent supports several Extended SMTP (ESMTP) settings. These are settings which might or might not be supported by another SMTP system.

The following ESMTP extensions are supported:

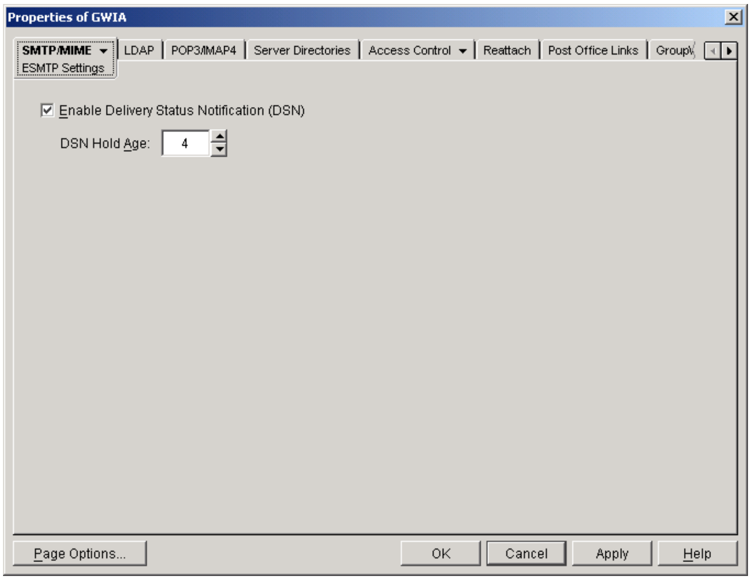
- **SIZE** For more information, see RFC 1870 (http://www.ietf.org/rfc/rfc1870.txt).
- **AUTH** For more information, see RFC 2554 (http://www.ietf.org/rfc/rfc2554.txt).
- **DSN** For more information, see RFC 3464 (http://www.ietf.org/rfc/rfc3464.txt) and RFC 3461 (http://www.ietf.org/rfc/rfc3461.txt).

- **8BITMIME** For more information, see RFC 1652 (http://www.ietf.org/rfc/rfc1652.txt).
- **STARTTLS** For more information, see RFC 3207 (http://www.ietf.org/rfc/rfc3207.txt).

To configure ESMTP settings:

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click SMTP/MIME > ESMTP Settings.



☑ Enable Delivery Status Notification (DSN)

DSN Hold Age: 4

3 Fill in the fields:

Enable Delivery Status Notification: Turn on this option to allow the Internet Agent to request status notifications for outgoing messages and to supply status notifications for incoming messages. This requires the external e-mail system to also support Delivery Status Notification. Currently, notification consists of two delivery statuses: successful or unsuccessful.

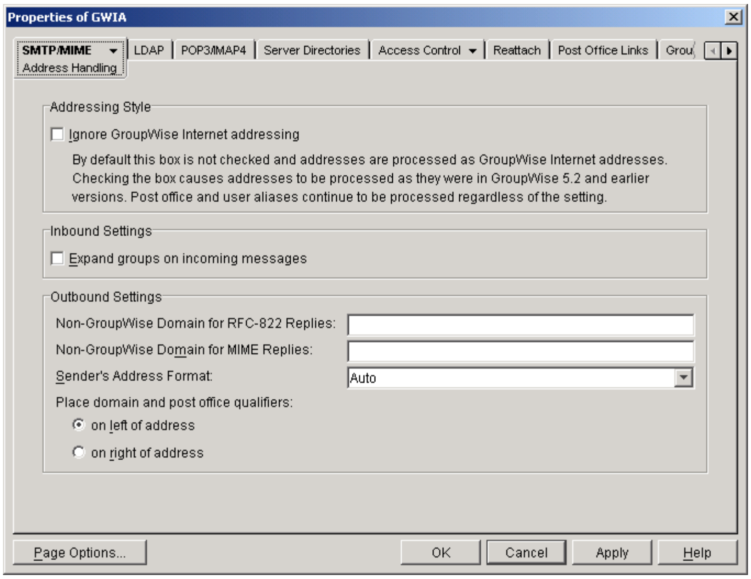
If you enable the Delivery Status Notification option, you need to select the number of days that you want the Internet Agent to retain information about the external sender so that status updates can be delivered to him or her. For example, the default hold age causes the sender information to be retained for 4 days. If the Internet Agent does not receive delivery status notification from the GroupWise recipient's Post Office Agent (POA) within that time period, it deletes the sender information and the sender does not receive any delivery status notification.

4 Click OK to save the changes.

Configuring How the Internet Agent Handles E-Mail Addresses

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click SMTP/MIME > Address Handling.



Addressing Style

□ Ignore GroupWise Internet addressing

By default this box is not checked and addresses are processed as GroupWise Internet addresses. Checking the box causes addresses to be processed as they were in GroupWise 5.2 and earlier versions. Post office and user aliases continue to be processed regardless of the setting.

Inbound Settings

□ Expand groups on incoming messages

Outbound Settings

Non-GroupWise Domain for RFC-822 Replies:

Non-GroupWise Domain for MIME Replies:

Sender's Address Format: Auto

Place domain and post office qualifiers:

● on left of address

○ on right of address

3 Fill in the fields:

Ignore GroupWise Internet Addressing: GroupWise supports both Internet-style addressing (*user@host*) and GroupWise proprietary addressing (*user_ID.post_office.domain*). By default, the Internet Agent uses Internet-style addressing.

If you do not want the Internet Agent to use standard Internet-style addressing (*user@host*), turn on the Ignore GroupWise Internet Addressing option. With this option turned on, messages use the mail domain name in the Foreign ID field (GroupWise tab > Identification page) for the domain portion of a user's Internet address. If you've included multiple mail domain names in the Foreign ID field or the frgnames.cfg file, as described in "Listing Foreign Domain Names" on page 666, the first mail domain name listed will be the one used in addresses.

The Internet Agent will support user and post office aliases in either mode. This setting corresponds with the Internet Agent's /dia switch.

Expand Groups on Incoming Messages: Turn on this option to have incoming Internet messages addressed to public groups sent to all members of the groups. This setting corresponds with the Internet Agent's /group switch.

Non-GroupWise Domain for RFC-822 Replies: This setting can be used only if 1) you created a non-GroupWise domain to represent all or part of the Internet, and 2) you defined the non-GroupWise domain's outgoing conversion format as RFC-822 when you linked the Internet Agent to the domain.

Enter the name of the non-GroupWise domain associated with the RFC-822 conversion format. When a GroupWise user replies to a message that was originally received by the Internet Agent in RFC-822 format, the reply is sent to the specified non-GroupWise domain and converted to RFC-822 format so that it is in the same format as the original message.

This setting corresponds with the Internet Agent's /fd822 switch.

Non-GroupWise Domain for MIME Replies: This setting can be used only if 1) you've created a non-GroupWise domain that represents all or part of the Internet, and 2) you defined the non-GroupWise domain's outgoing conversion format as MIME when you linked the Internet Agent to the domain.

Enter the name of the non-GroupWise domain associated with the MIME conversion format. When a GroupWise user replies to a message that was originally received by the Internet Agent in MIME format, the reply is sent to the specified non-GroupWise domain and converted to MIME format so that it is in the same format as the original message.

This setting corresponds with the Internet Agent's /fdmime switch.

Sender's Address Format: This setting applies only if you have not enabled GroupWise Internet addressing (in other words, you've selected the Ignore GroupWise Internet Addressing option). If GroupWise Internet addressing is enabled, the Internet Agent ignores this setting and uses the preferred address format established for outbound messages (Tools menu > GroupWise System Operations > Internet Addressing).

The Sender's Address Format setting lets you specify which GroupWise address components (*domain.post_office.user_ID*) will be included as the user portion of the address on outbound messages. You can choose from the following options:

- **Domain, Post Office, User, and Hostname:** Uses the *domain.post_office.user_ID@host* syntax.
- **Post Office, User, and Hostname:** Uses the *post_office.user_ID@host* syntax.
- **User and Hostname:** Uses the *user_ID@host* syntax.
- **Auto (default):** Uses the GroupWise addressing components required to make the address unique within the user's GroupWise system. If a user ID is unique in a GroupWise system, the outbound address will use only the user ID. If the post office or domain.post office components are required to make the address unique, these components will also be included in the outbound address.

The Sender's Address Format setting corresponds with the Internet Agent's /aql switch.

Place Domain and Post Office Qualifiers: If the sender's address format must include the domain and/or post office portions to be unique, you can use this option to determine where the domain and post office portions are located within the address.

- **On Left of Address (default):** Leaves the domain and post office portions on the left side of the @ sign (for example, *domain.post_office.user_ID@host*.
- **On Right of Address:** Moves the domain and post office portions to the right side of the @ sign, making the domain and post office part of the host portion of the address (for example, *user_ID@post_office.domain.host*. If you choose this option, you must ensure that your DNS server can resolve each *post_office.domain.host* portion of the address. This setting corresponds with the Internet Agent's /aqor switch.

4 Click OK to save the changes.

Listing Foreign Domain Names

The Foreign ID field (ConsoleOne > Internet Agent object > GroupWise tab > Identification page) identifies the Internet domain names for which the Internet Agent will accept messages. The field should always include your mail domain name (for example, novell.com). You can include additional domain names by separating them with a space, as in the following example:

```
novell.com gw.novell.com gwia.novell.com
```

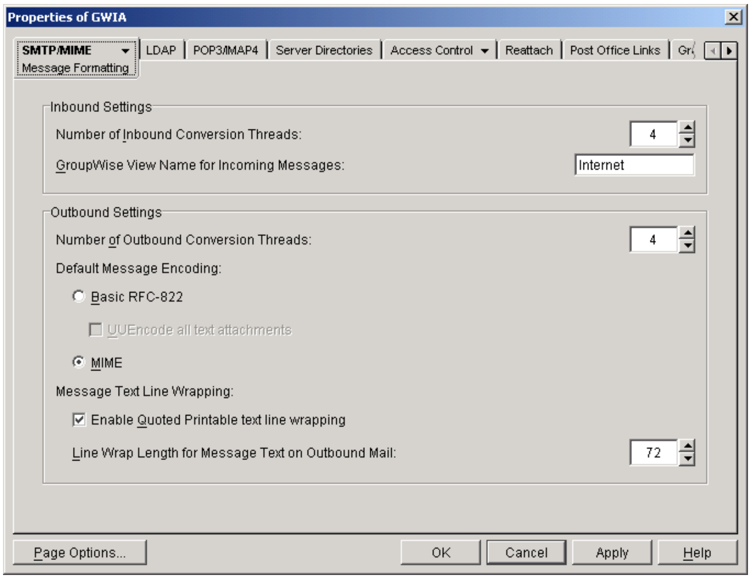
When you list multiple Internet domain names, the Internet Agent accepts messages for a GroupWise user provided any of the Internet domain names are used (for example, jsmith@novell.com, jsmith@gw.novell.com, or jsmith@gwia.novell.com).

The field limit is 255 characters. If you need to exceed that limit, you can create a frgnames.cfg text file in the *domain*\wpgate*gwia* directory. Include each Internet domain name, separated by a space, just like you would in the Foreign ID field.

Determining Format Options for Messages

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click SMTP/MIME > Message Formatting.



Inbound Settings

Number of Inbound Conversion Threads: 4

GroupWise View Name for Incoming Messages: Internet

Outbound Settings

Number of Outbound Conversion Threads: 4

Default Message Encoding:

○ Basic RFC-822

□ UUEncode all text attachments

● MIME

Message Text Line Wrapping:

☑ Enable Quoted Printable text line wrapping

Line Wrap Length for Message Text on Outbound Mail: 72

3 Fill in the fields:

Number of Inbound Conversion Threads: The inbound conversion threads setting lets you specify the number of threads that will convert inbound messages from MIME or RFC-822 format to the GroupWise message format. The default setting is 4. This setting corresponds with the Internet Agent's /rt switch.

GroupWise View Name for Incoming Messages: The GroupWise view setting lets you specify a mail view attachment for all inbound Internet messages. A view is the screen that a user sees when a message is opened. This switch helps users identify Internet messages. If you do not specify a view, or if the view has not been configured, the default view (Internet) will be used. This setting corresponds with the Internet Agent's /mv switch.

Number of Outbound Conversion Threads: The outbound conversion threads setting lets you specify the number of threads that will convert outbound messages from the GroupWise message format to MIME or RFC-822 format. The default setting is 4. This setting corresponds with the Internet Agent's /st switch.

Default Message Encoding: The default message encoding setting lets you select the encoding method for your outbound Internet messages. You can select either Basic RFC-822 formatting or MIME formatting. MIME is the default message format. This setting corresponds with the Internet Agent's /mime switch.

If you select the Basic RFC-822 option, you can decide whether or not to have the Internet Agent UUEncode all ASCII text attachments to RFC-822 formatted messages. By default, this option is turned off, which means ASCII text attachments will be included as part of the message body. By default, the setting is off. This setting corresponds with the Internet Agent's /uueaa switch.

Message Text Line Wrapping: The Quoted Printable text line wrapping setting lets you select the Quoted Printable MIME standard for line wrapping. By default this setting is turned on. If you turn the setting off, MIME messages will go out as plain text and will wrap text according to the number of characters specified in the line wrap length setting. This setting corresponds with the Internet Agent's /nqpmt switch.

The Line Wrap Length for Message Text on Outbound Mail setting lets you specify the line length for outgoing messages. This is useful if the recipient's e-mail system requires a certain line length. The default line length is 72 characters. This setting corresponds with the Internet Agent's /wrap switch.

4 Click OK to save the changes.

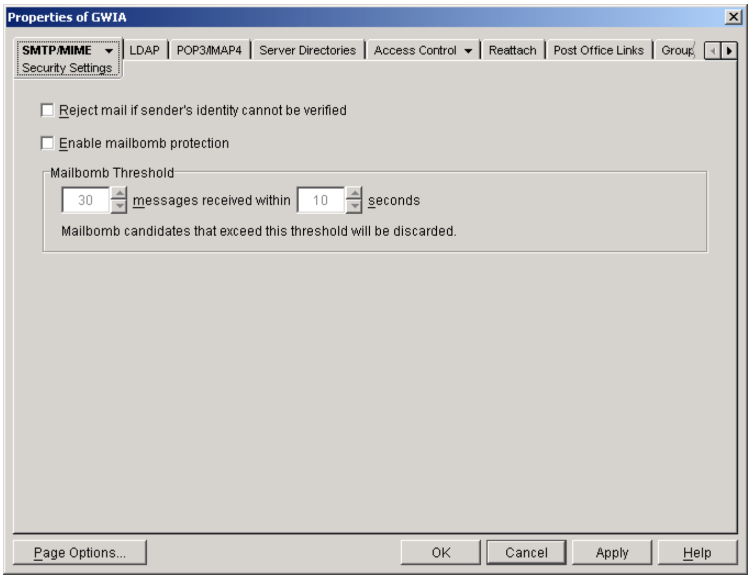
Protecting Against Unidentified Hosts and Mailbombs (Spam)

Multiple unsolicited messages (sometimes called a *mailbomb* or *spam*) from the Internet can potentially harm your GroupWise messaging environment. You can use the settings on the SMTP Security page to help protect your GroupWise system from malicious or accidental attacks.

To configure the SMTP security settings:

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click SMTP/MIME > Security Settings.



□ Reject mail if sender's identity cannot be verified

□ Enable mailbomb protection

Mailbomb Threshold

30 messages received within 10 seconds

Mailbomb candidates that exceed this threshold will be discarded.

3 Fill in the fields:

Reject Mail if Sender's Identity Cannot be Verified: This setting lets you prevent messages if the sender's host is not authentic.

When this setting is turned on, the Internet Agent will refuse messages from a smart host if a DNS reverse lookup shows that a "PTR" record does not exist for the IP address of the sender's host.

When this setting is turned off, the Internet Agent will accept messages from any host, but display a warning if the initiating host is not authentic.

This setting corresponds with the Internet Agent's /rejbs switch.

Enable Mailbomb Protection: Mailbomb protection is turned off by default. You can turn it on by clicking the check box.

Mailbomb Threshold: When you enable Mailbomb protection, default values are defined in the threshold settings. The default settings are 30 messages received within 10 seconds. You can change the settings to establish an acceptable security level.

Any group of messages that exceeds the specified threshold settings will be entirely discarded. If you want to prevent future mailbombs from the mailbomb sender, identify the sender's IP address (by looking at the Internet Agent's console) and then modify the appropriate class of service to prevent mail being received from that IP address (Access Control tab > Settings page).

The time setting corresponds with the Internet Agent's /mbtime switch. The message count setting corresponds with the /mbcount switch.

4 Click OK to save the changes.

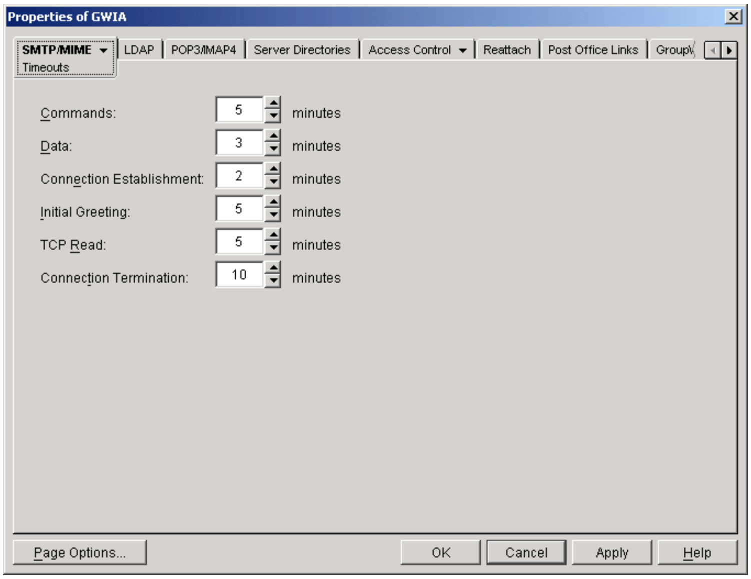
Configuring the SMTP Timeout Settings

The SMTP Timeout settings specify how long the Internet Agent's SMTP service will wait to receive data that it can process. After the allocated time expires, the Internet Agent might give a TCP read/write error.

To configure the SMTP timeout settings:

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click SMTP/MIME > Timeouts.



Commands: 5 minutes

Data: 3 minutes

Connection Establishment: 2 minutes

Initial Greeting: 5 minutes

TCP Read: 5 minutes

Connection Termination: 10 minutes

3 Fill in the fields:

Commands: The Commands setting lets you specify how long the Internet Agent will wait for an SMTP command. The default is 5 minutes. This setting corresponds with the Internet Agent's /tc switch.

Data: The Data setting lets you specify how long the Internet Agent will wait for data from the receiving host. The default is 3 minutes. This setting corresponds with the Internet Agent's /td switch.

Connection Establishment: The Connection Establishment setting lets you specify how long the Internet Agent will wait for the receiving host to establish a connection. The default is 2 minutes. This setting corresponds with the Internet Agent's /te switch.

Initial Greeting: The Initial Greeting setting lets you specify how long the Internet Agent will wait for the initial greeting from the receiving host. The default is 5 minutes. This setting corresponds with the Internet Agent's /tg switch.

TCP Read: The TCP Read setting lets you specify how long the Internet Agent will wait for a TCP read. The default is 5 minutes. This setting corresponds with the Internet Agent's /tr switch.

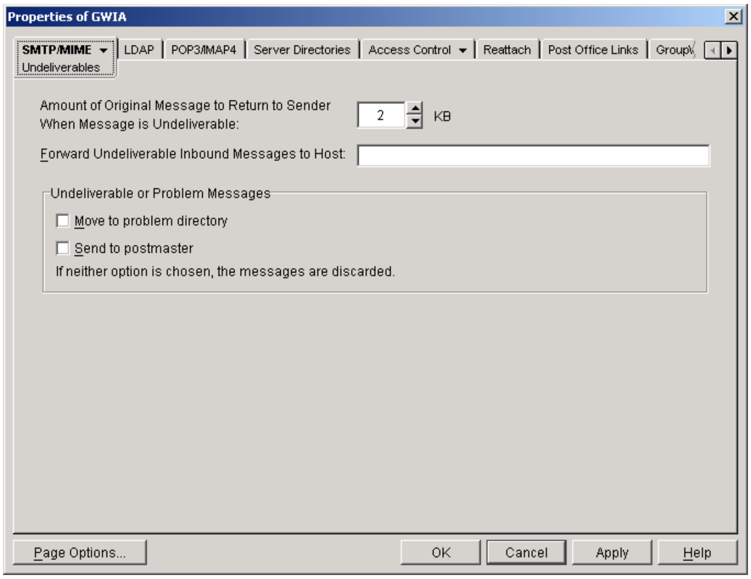
Connection Termination: The Connection Termination setting lets you specify how long the Internet Agent will wait for the receiving host to terminate the connection. The default is 10 minutes. This setting corresponds with the Internet Agent's /tt switch.

4 Click OK to save the changes.

Determining What to Do with Undeliverable Messages

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click SMTP/MIME > Undeliverables.



Amount of Original Message to Return to Sender When Message is Undeliverable: 2 KB

Forward Undeliverable Inbound Messages to Host:

Undeliverable or Problem Messages

□ Move to problem directory

□ Send to postmaster

If neither option is chosen, the messages are discarded.

3 Fill in the fields:

Amount of Original Message to Return to Sender When Message is Undeliverable: This setting lets you specify how much of the original message is sent back to the sender when a message is deemed undeliverable. By default, only 2 KB of the original message will be sent back. This setting corresponds with the Internet Agent's /mudas switch.

Forward Undeliverable Inbound Messages to Host: This setting lets you specify a host that will be forwarded undeliverable messages. This may be useful if you use UNIX sendmail aliases.

When an IP address is specified rather than a DNS hostname, the IP address must be surrounded by square brackets [ ]. For example, [151.155.134.246].

This setting corresponds with the Internet Agent's /fut switch.

Undeliverable or Problem Messages: This setting lets you specify what you want the Internet Agent to do with problem messages. A problem message is an inbound or outbound message that the Internet Agent cannot convert properly. By default, problem messages are discarded. If you want to save problem messages, specify whether to move the messages to the problem directory (gwprob), send them to the postmaster, or do both. This setting corresponds with the Internet Agent's /badmsg switch.

IMPORTANT: Despite the field name (Undeliverable or Problem Messages), this setting does not apply to undeliverable messages.

4 Click OK to save the changes.

Configuring SMTP Dial-Up Services

SMTP dial-up services can be used when you don't require a permanent connection to the Internet and want to periodically check for mail messages queued for processing. Perform the following tasks in order to use SMTP dial-up services:

- "Setting up Internet Dial-Up Software" on page 671
- "Enabling Dial-Up Services" on page 671
- "Creating a Dial-Up Schedule" on page 672

Setting up Internet Dial-Up Software

The Internet Agent requires routing software to make the dial-up connection to the Internet. The Internet Agent cannot make this connection itself; it simply creates packets to hand off to the routing software.

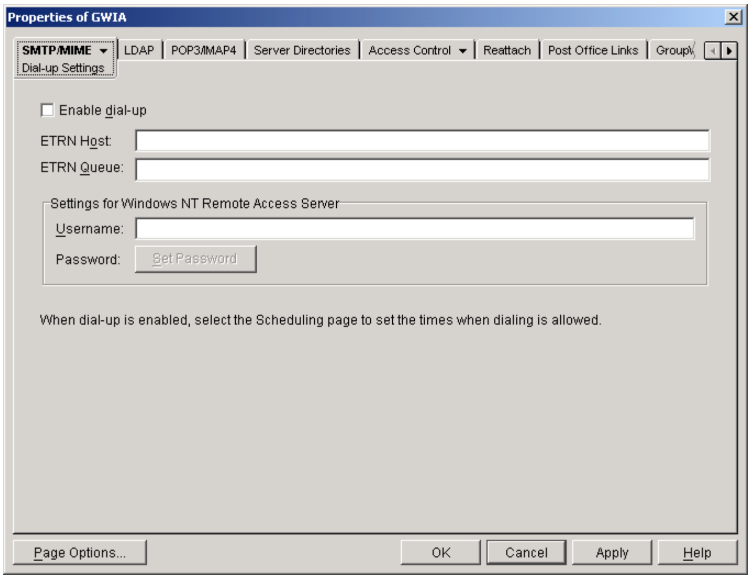
For information about configuring the Internet Agent's dial-up feature with routing software, see Novell Technical Information Document 10007366 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10007366.htm).

Enabling Dial-Up Services

After you have the appropriate routing software in place, you can enable and configure the Internet Agent's dial-up services.

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click SMTP/MIME > Dial-Up Settings.



☐ Enable dial-up

ETRN Host:

ETRN Queue:

Settings for Windows NT Remote Access Server

Username:

Password: Set Password

When dial-up is enabled, select the Scheduling page to set the times when dialing is allowed.

3 Fill in the fields:

Enable Dial-Up: Turn on this option to allow the Internet Agent to support SMTP dial-up service. This option is off by default. This setting corresponds with the Internet Agent's /usedialup switch.

ETRN Host: Specify the IP address, or DNS hostname, of the mail server (where your mail account resides) at your Internet Service Provider. You should obtain this address from your Internet Service Provider. This setting corresponds with the Internet Agent's /etrnhost switch.

ETRN Queue: Specify your e-mail domain as provided by your Internet Service Provider (for example, novell.com). This setting corresponds with the Internet Agent's /etrnqueue switch.

Username: The Username setting applies only if you are using a Windows NT Remote Access Server (RAS) and the Internet Agent is not running on the same server as the RAS.

Specify the RAS Security username. This setting corresponds with the Internet Agent's /dialuser switch.

Password: The Password setting applies only if you are using a Windows NT Remote Access Server (RAS) and the Internet Agent is not running on the same server as the RAS.

Specify the RAS Security user's password. This setting corresponds with the Internet Agent's /dialpass switch.

4 Click OK to save the changes.

Creating a Dial-Up Schedule

After you've enabled the Internet Agent to use a dial-up connection, you need to schedule the times when the Internet Agent will initiate a connection.

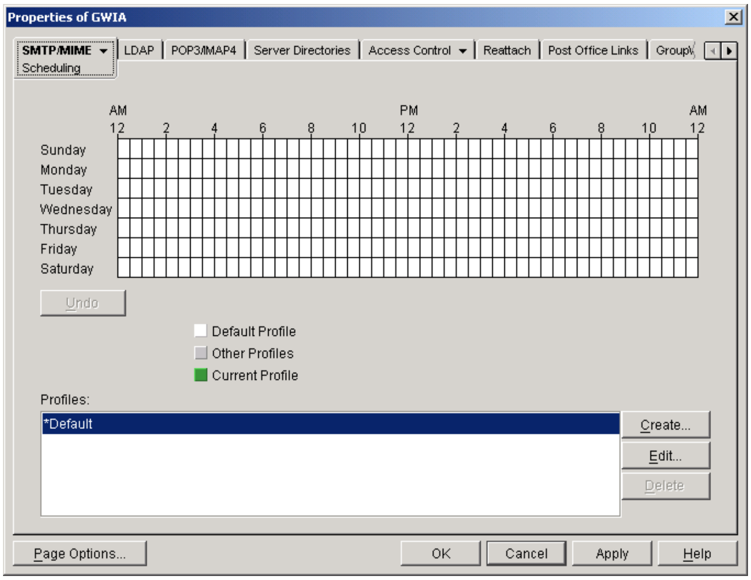
NOTE: When the Internet Agent initiates a connection, it simply passes TCP/IP packets to the routing service that makes the Internet connection. The routing software, not the Internet Agent, is responsible for the actual dial-up or timeout.

The Internet Agent uses profiles to enable you to assign different dial-up criteria to different times. For example, the default profile instructs the Internet Agent to initiate a dial-up connection whenever an outgoing message is placed in its send queue. However, during the night, you may want the Internet Agent to initiate a connection only after 30 outgoing messages have been queued.

In this case, you could create a profile that requires 30 messages to be queued and then apply the profile between the hours of 11 p.m. and 7 a.m. each day.

To create a dial-up schedule:

1. In ConsoleOne, right-click the Internet Agent object, then click Properties.
2. Click SMTP/MIME > Scheduling.



3. To apply a profile to a block of time, skip to "Applying a Profile" on page 673.

   or

   To create a profile, skip to "Creating a Profile" on page 673.

   or

   To edit a profile, skip to "Editing a Profile" on page 674.

   or

   To delete a profile, skip to "Deleting a Profile" on page 674

Applying a Profile

1. Select the profile in the Profiles list.
2. Click the desired hour.

   or

   Drag to select multiple hours.
3. Click Apply to save the changes or click OK to save the changes and close the page.

Creating a Profile

1. Click Create to display the Create Profile dialog box.
2. Fill in the fields:

   Name: Enter a unique name for the profile. It must be different than any other name in the Profile list.

Description: If desired, enter a description for the profile.

Queue Thresholds: The queue thresholds determine the criteria for the Internet Agent to initiate a dial-up connection to send messages. The settings do not apply to receiving messages (see Dial Parameters below).

You can base the criteria on the number of messages in the send queue, the total size of the messages in the send queue, or the number of minutes to wait between connections. If necessary, you can use a combination of the three criteria.

For example, if you set Messages to 20, Kilobytes to 100, and Minutes to 60, the Internet Agent will instruct the routing service to initiate a dial-up connection when 20 messages have accumulated in the queue, when the total size of the messages in the queue reaches 100K, or when 60 minutes have passed since the last connection.

Dial Parameters: The dial parameters serve two purposes: 1) the Internet Agent passes the Redial Interval and Idle Time Before Hangup parameters to the routing service to use when initiating a connection to send outbound messages, and 2) the Internet Agent uses the Polling Interval parameter to determine how often the routing service should initiate a connection to check for inbound messages. The Polling Interval parameter is required.

Specify the interval between redials (default is 30 seconds), the amount of time to wait before hanging up when there are no messages to process (default is 60 seconds), and the interval between polling for inbound messages (default is 0 minutes).

3. Click OK to add the profile to the Profiles list.
4. To apply the profile to a block of time, see "Applying a Profile" on page 673.

Editing a Profile

1. Select the profile you want to edit, then click Edit to display the Edit Profile dialog box.
2. Modify the desired fields. For information about each of the fields, click the Help button in the Edit Profile dialog box or see "Creating a Profile" on page 673.
3. Click Apply to save the changes or click OK to save the changes and close the page.

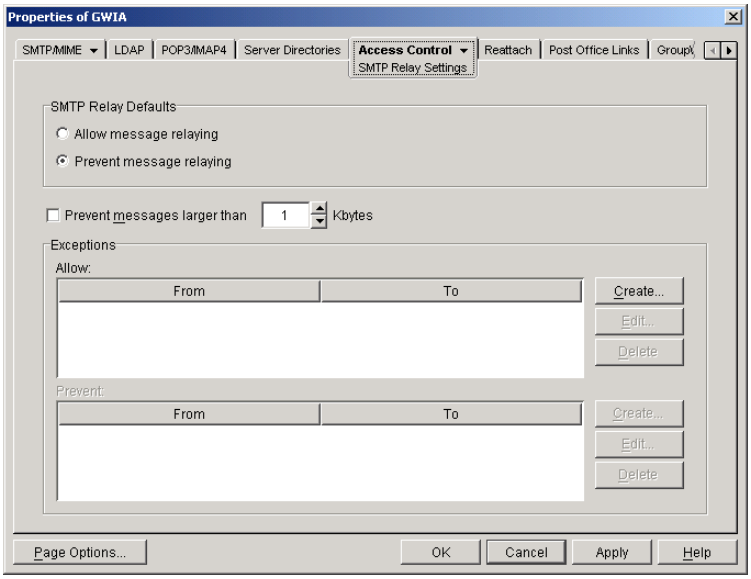
Deleting a Profile

1. Select the profile you want to remove from the list, then click Delete.
2. Click Apply to save the changes or click OK to save the changes and close the page.

Enabling SMTP Relaying

You can enable the Internet Agent to function as a relay host for Internet messages. The Internet Agent can relay messages received from all Internet hosts, or you can select specific hosts for which you will allow it to relay.

1. In ConsoleOne, right-click the Internet Agent object, then click Properties.
2. Click Access Control > SMTP Relay Settings.



SMTP Relay Defaults

○ Allow message relaying

● Prevent message relaying

□ Prevent messages larger than 1 Kbytes

Exceptions

Allow:

From	To

Prevent:

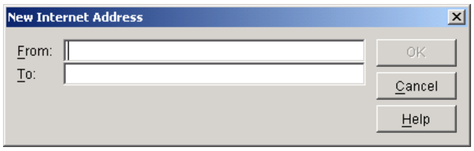
From	To

3 Under SMTP Relay Defaults, select whether you want to allow or prevent message relaying.

If you prevent message relaying, you can define exceptions that will allow message relaying for specific Internet hosts. This can also be done if you allow message relaying. We suggest that you select the option that enables you to define the fewest exceptions.

4 To prevent relaying of messages larger than a specific size (regardless of the SMTP Relay Defaults setting), enable the Prevent Messages Larger Than option and specify the size limitation.

5 To define an exception, click Create to display the New Internet Address dialog box.



From:

To:

6 Fill in the following fields:

From: Enter the Internet address that must be in the message's From field for the exception to be applied.

To: Enter the Internet address that must be in the message's To field for the exception to be applied. This is also the address that the message will be relayed to (in the case of an Allow exception).

In both the From and To fields, you can use either an IP address or a DNS hostname, as shown in the following examples:

```
novell.com
10.1.1.10
```

You can enter a specific address, as shown above, or you can use wildcards and IP address ranges to specify multiple addresses, as follows:

```
*.novell.com
10.1.1.*
10.1.1.10-15
```

7. Click OK to add the exception to the list.
8. When finished defining exceptions, click OK to save your changes.

Configuring SMTP Host Authentication

The Internet Agent supports SMTP host authentication for both outbound and inbound message traffic.

Outbound Authentication

For outbound authentication to other SMTP hosts, the Internet Agent requires that the remote SMTP hosts support the AUTH LOGIN authentication method. To set up outbound authentication:

1. Include the remote SMTP host's domain name an authentication credentials in the gwauth.cfg file, located in the *domain*\wpgate\gwia directory. The format is:

   ```
   domain_name   authuser   authpassword
   ```

   For example:

   ```
   smtp.novell.com   remotehost   novell
   ```

2. If you have multiple SMTP hosts that require authentication before they will accept messages from your system, create an entry for each host. Make sure to include a hard return after the last entry.
3. If you want to allow the Internet Agent to send messages only to SMTP hosts listed in the gwauth.cfg file, use the following startup switch:

   ```
   /forceoutboundauth
   ```

   With this option enabled, if a message is sent to an SMTP host not listed in the gwauth.cfg file, the sender will receive an Undeliverable message.

Inbound Authentication

For inbound authentication from other SMTP hosts, you can use the /forceinboundauth startup switch to ensure that the Internet Agent accepts messages only from SMTP hosts that use the AUTH LOGIN authentication method to provide a valid GroupWise user ID and password. The remote SMTP hosts can use any valid GroupWise user ID and password. However, for security reasons, we recommend that you create a dedicated GroupWise user account for remote SMTP host authentication.

Using a Route Configuration File

The Internet Agent supports the use of a route configuration file (route.cfg) to specify destination SMTP hosts. This can be useful in situations such as the following:

- You are using a relay host for outbound messages. However, you want some outbound messages sent directly to the destination host rather than the relay host. Whenever a message is addressed to a user at a host that is included in the route.cfg file, the Internet Agent will send the message directly to the destination host rather than the relay host.
- You need to send messages to SMTP hosts that are unknown to the public Domain Name Servers. The route.cfg file acts much like a hosts file to enable the Internet Agent to resolve addresses not listed in DNS.
- You want to route messages through an SMTP host that checks for viruses (or performs some other task) before routing them to the destination host.

To set up a route.cfg file:

1. Create the route.cfg file as a text file in the *domain*\wpgate*gwia* directory.
2. Add an entry for each SMTP host you want to send to directly. The entry format is:

   ```
   hostname  address
   ```

   where *address* is either an alternative hostname or an IP address. For example:

   ```
   novell.com gwia.novell.com
   unixbox [123.1.2.3]
   ```

   Make sure to include a hard return after the last entry. In addition, if you use an IP address, it must be included in square brackets, as shown in the second example.
3. Save the route.cfg file.

Customizing Delivery Status Notifications

The Internet Agent returns status messages for all outbound messages. For example, if a GroupWise user sends a message that the Internet Agent cannot deliver, the Internet Agent returns an undeliverable message to the GroupWise user.

By default, the Internet Agent uses internal status messages. However, you can override the internal status messages by using a status.xml file that includes the status messages you want to use.

1. Open the appropriate status*xx*.xml file, located in the *domain*\wpgate*gwia* directory.

   The *domain*\wpgate*gwia* directory includes a status*xx*.xml file for each language included on your *GroupWise 6.5 Administrator* CD (for example, statusus.xml, statusde.xml, and statusfr.xml).
2. Make the modifications you want.

   The following sample code shows the elements and default text of the Undeliverable Message status:

   ```
   <STATUS_MESSAGE type="undeliverableMessage" xml:lang="en-US">
   <SUBJECT>Message status - undeliverable</SUBJECT>
   <MESSAGE_BODY>
   <TEXT>\r\nThe attached file had the following undeliverable
   recipient(s):\r\n</TEXT>
   <RECIPIENT_LIST format="\t%s\r\n"
   <SESSION_TRANSCRIPT>
   <TEXT>\r\nTranscript of session follows:\r\n<TEXT>
   </SESSION_TRANSCRIPT>
   <ATTACH_ORIGINAL_MSG></ATTACH_ORIGINAL_MSG>
   </MESSAGE_BODY>
   </STATUS_MESSAGE>
   ```

   You can modify text in the <SUBJECT> tag or in the <TEXT> tags.

   You can add additional <TEXT> tags in the <MESSAGE_BODY>.

   You can remove tags to keep an element from being displayed. For example, you could remove the <ATTACH_ORIGINAL_MSG></ATTACH_ORIGINAL_MSG> tags to keep the original message from displaying.

   You can use the following format characters and variables:

   - \t: tab

    - \r: carriage return
    - \n: line feed
    - %s: recipient name variable

3. Save the file, renaming it from status*xx*.xml to status.xml.
4. Restart the Internet Agent.

The Internet Agent will now use the status messages defined in the status.xml file rather than its internal status messages.

Managing MIME Messages

Multipurpose Internet Mail Extensions, or MIME, provides a means to interchange text in languages with different character sets. Multimedia e-mail can be sent between different computer systems that use the SMTP protocol. MIME allows you to send and receive e-mail messages containing:

- Images
- Sounds
- UNIX Tar Files
- PostScript*
- FTP-able File Pointers
- Non-ASCII Character Sets
- Enriched Text
- Nearly any other file

Because MIME handles such a variety of file types, you might need to customize aspects of MIME for your users.

- "Customizing MIME Preamble Text" on page 678
- "Customizing MIME Content-Type Mappings" on page 679

Customizing MIME Preamble Text

An ASCII file called preamble.txt is installed in the Internet Agent gateway directory (*domain*\wpgate*gwia*). This file, which is included with any MIME multipart message, is displayed when the message recipient lacks a MIME-compliant mail reader.

The content of the preamble.txt file is a warning, in English, that the file is being sent in MIME format. If the recipient cannot read the message, he or she will need to either use a MIME-compliant mail reader or reply to the sender and request the message not be sent in MIME format.

It is recommended that you use the preamble.txt file so that those who read MIME messages coming from your GroupWise system and who lack MIME-compliant mail readers will understand why they cannot read the message and will be able to take corrective action.

If you choose to modify the preamble.txt file, be aware of the following considerations:

- The maximum file size is 1024 bytes (1 KB)
- This file is read by the Internet Agent when the Internet Agent starts, so if you change the file, you will need to restart the Internet Agent.

The Internet Agent's gateway directory also contains a preamble.all file. The preamble.all file includes the text of preamble.txt translated into several languages. If you anticipate that your users will be sending mail to non-English speaking users, you may want to copy the appropriate language sections from the preamble.all file to the preamble.txt file.

The 1024-byte limit on the size of the preamble.txt file still applies, so make sure that the file does not exceed 1024 bytes.

Customizing MIME Content-Type Mappings

By default, the GroupWise client determines the MIME content-type and encoding for message attachments. If, for some reason, the GroupWise client cannot determine the appropriate MIME content-type and encoding for an attachment, the Internet Agent must determine the content-type and encoding.

The Internet Agent uses a mimetype.cfg file to map attachments to the appropriate MIME content types. Based on an attachment's content type, the Internet Agent encodes the attachment using quoted-printable, Base64, or BinHex. Generally, quoted-printable is used for text-based files, Base64 for application files, and BinHex for Macintosh files.

The mimetype.cfg file includes mappings for many standard files. If necessary, you can modify the file to include additional mappings. If an attachment is sent which does not have a mapping in the file, the Internet Agent will choose quoted-printable, BinHex or Base64 encoding.

The mimetype.cfg file is also used for RFC-822 attachments, but UUencode or BinHex encoding will be used regardless of the mapped content type.

The mimetype.cfg file is located in the *domain*\wpgate*gwia* directory. The following section provide information you will need to know to modify the file:

- "Mapping Format" on page 679
- "File Organization" on page 680

Mapping Format

Each mapping entry in the file uses the following format:

```
content-type .ext|dtk-code|mac-ttttcccc [/parms] ["comment"]
```

Element	Description
content-type	The MIME content type to which the file type is being mapped (for example, text/plain). You can omit the content-type only if you use the /parms element to explicitly define the encoding scheme for the file type.

Element	Description
.ext|dtk-*code*|mac-*ttttcccc*	The .ext element, dtk-*code* element, and mac-*ttttcccc* element are mutually exclusive. Each entry will contain only one of the elements. ◆ **.ext:** The file type extension being mapped to the content type (for example, .txt). ◆ **dtk-*code*:** The detect code being mapped to the content type (for example, dtk-1126). GroupWise assigns a detect code to each attachment type. ◆ **mac-*ttttcccc*:** The Macintosh file type and creator application being mapped to the content type (for example, mac-textmswd). The first four characters (*tttt*) are used for the file type. The last four characters (*cccc*) are used for the creator application. You can use ???? for the creator portion (mac-text????) to indicate a certain file type created by any application. You can use ???? in both portions (mac-????????) to match any file type created by any application.
/parms	Optional parameters that can be used to override the default encoding assigned to the MIME content type. Possible parameters are: ◆ /alternate ◆ /parallel ◆ /base64 ◆ /quoted-printable ◆ /quoted-printable-safe ◆ /uuencode ◆ /plain ◆ /binhex ◆ /nofixeol ◆ /force-*ext* ◆ /noconvert ◆ /apple-single ◆ /apple-double
"comment"	Optional content description

File Organization

The mimetype.cfg file contains the following four sections:

- [Parameter-Override]
- [Mac-Mappings]
- [Detect-Mappings]
- [Extension-Mappings]

[Parameter-Override]

The [Parameter-override] section take priority over other sections. You can use this section to force the encoding scheme for certain file types. This section also contains defaults for sending various kinds of multipart messages. This is how the Internet Agent knows to put attachments into MIME Alternate/Parallel multiparts.

[Mac-Mappings]

The [Mac-mappings] section defines mappings for Macintosh file attachments. The following is a sample entry:

```
application/msword mac-wdbnmswd "Word for Macintosh"
```

Macintosh files have a type and creator associated with them. The first four characters are used for the type and the last four characters are used for the creator application.

In the above example, the type is `wdbn` and the creator application is `mswd`. When a user attaches a Macintosh file to a message, the Internet Agent uses the appropriate entry in the [Map-mappings] section to map the file to a MIME content type and then encode the file according to the assigned encoding scheme. Unless otherwise specified by the /parms element, BinHex 4.0 will be used for the encoding. The following example shows how you can use the /parms element to change the encoding from the default (BinHex) to Base64:

```
application/msword mac-wdbnmswd /base64 "Word for Macintosh"
```

If necessary, you can use ???? for the creator portion (mac-text????) to indicate a certain file type created by any application. Or, you can use ???? in both portions (mac-????????) to match any file type created by any application. For example:

```
application/octet-stream mac-???????? /base64 "Mac Files"
```

This causes all Macintosh files to be encoded using Base64 rather than BinHex.

[Detect-Mappings]

GroupWise attempts to assign each attachment a detect code based on the attachment's file type. The [Detect-mappings] section defines the mappings based on these detect codes. The following is a sample entry:

```
application/msword dtk-1000 "Microsoft Word 4"
```

The Internet Agent will use the detect code to map to a MIME content type and then encode the file according to the assigned encoding scheme. If there is no mapping specified or if the file type cannot be determined, one of the other mapping methods, such as Extension-Mappings, will be used. The detect codes associated with attachments are GroupWise internal codes and cannot be changed.

[Extension-Mappings]

If a mapping could not be made based on the entries in the [Mac-mappings] and [Detect-mappings] section, the Internet Agent uses the [Extension-mappings] section. The [Extension-mappings] section defines mappings based on the attachment's file extension. The following is a sample entry:

```
application/pdf .pdf
```

Configuring LDAP Services

The Internet Agent supports the Lightweight Directory Access Protocol (LDAP) standard. With LDAP enabled, the GroupWise® Internet Agent functions as an LDAP server, allowing LDAP queries for GroupWise user information contained in the Novell® eDirectory™. You can also configure which GroupWise fields (Given Name, Last Name, Phone, and E-Mail) are visible to an LDAP query.

- "Enabling LDAP Services" on page 682
- "Configuring Public Access" on page 683

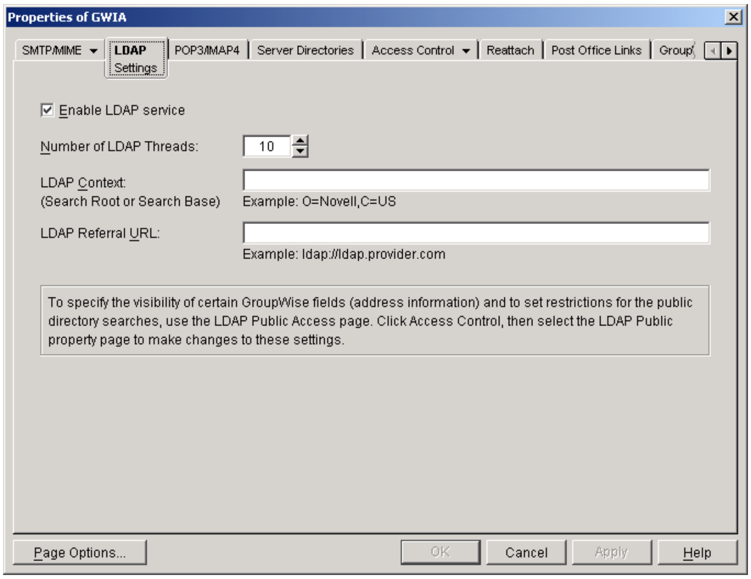
IMPORTANT: For users to perform LDAP searches for GroupWise user information, they need to define the GroupWise Address Book as a directory in their e-mail client. When doing so, they will use the Internet Agent's DNS hostname or IP address for the LDAP server address

Enabling LDAP Services

To enable and configure LDAP services for mail client access:

1 In ConsoleOne®, right-click the Internet Agent object, then click Properties.

2 Click LDAP > Settings to display the LDAP Settings page.



Properties of GWIA

☑ Enable LDAP service

Number of LDAP Threads: 10

LDAP Context:
(Search Root or Search Base)
Example: O=Novell,C=US

LDAP Referral URL:
Example: ldap://ldap.provider.com

To specify the visibility of certain GroupWise fields (address information) and to set restrictions for the public directory searches, use the LDAP Public Access page. Click Access Control, then select the LDAP Public property page to make changes to these settings.

3 Fill in the fields:

Enable LDAP Service: Turn on this option to allow LDAP queries. LDAP service is on by default. This setting corresponds to the Internet Agent's /ldap switch.

Number of LDAP Threads: The LDAP Threads setting lets you specify the maximum number of threads that will process LDAP queries. The default is 10 threads. This setting corresponds with the Internet Agent's /ldapthrd switch.

LDAP Context: Use this option to limit the directory context in which the LDAP server will search. For example, if you want to limit LDAP searches to the Novell organization container located under the United States country container, enter O=Novell,C=US. This setting corresponds with the Internet Agent's /ldapcntxt switch.

If you enter an LDAP context, you must make sure that users, when defining the directory in their e-mail client, enter the same context (using the identical text you did) in the Search Base or Search Root field.

You can leave the settings empty in both locations.

LDAP Referral URL: Use this option to define a secondary LDAP server to which you can refer an LDAP query if the query fails to find a user or address in your GroupWise system. For this option to work, the requesting Web browser must be able to track referral URLs. This setting corresponds with the Internet Agent's /ldaprefurl switch.

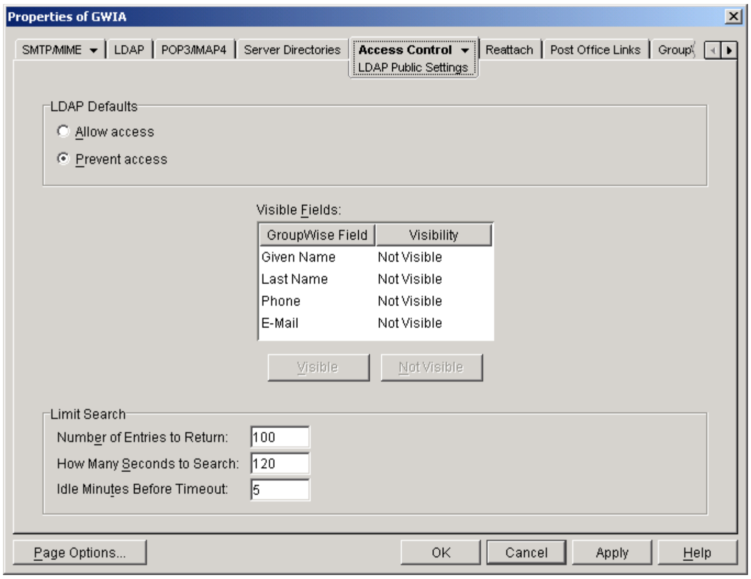
4 Continue with the next section, Configuring Public Access.

Configuring Public Access

After you've enabled LDAP services, you can configure which GroupWise fields will be visible to LDAP searches and also set search restrictions. By default, no fields are visible.

1 If the Internet Agent object's property page is not open, right-click the Internet Agent object, then click Properties.

2 Click Access Control > LDAP Public Settings.



Properties of GWIA

LDAP Defaults

○ Allow access

● Prevent access

Visible Fields:

GroupWise Field	Visibility
Given Name	Not Visible
Last Name	Not Visible
Phone	Not Visible
E-Mail	Not Visible

Limit Search

Number of Entries to Return: 100

How Many Seconds to Search: 120

Idle Minutes Before Timeout: 5

3 Fill in the fields:

LDAP Defaults: Select one of the following defaults for public access: Allow Access or Prevent Access. If you select Allow Access, the GroupWise fields (in the Visible Fields lists) will default to Visible for an LDAP search. If you select Prevent Access, the GroupWise fields will default to Not Visible.

Visible Fields: You can override the default visibility for a GroupWise field (Given Name, Last Name, Phone, and E-Mail) by selecting the field and then clicking the appropriate visibility button (Visible or Not Visible). For example, if you've selected Allow Access as the LDAP default, but you don't want users' telephone numbers to be visible, you can mark the Phone field as Not Visible.

Number of Entries to Return: Select the maximum number of entries to return. The default is 100.

How Many Seconds to Search: Select the maximum amount of time (in seconds) you want the Internet Agent to spend searching. The default is 120 seconds.

Idle Minutes before Timeout: Specify the number of minutes to allow the search to continue without finding a matching address entry. The default is 5 minutes.

4 Click OK to save the changes.

Configuring POP3/IMAP4 Services

The Post Office Protocol 3 (POP3) and the Internet Message Access Protocol 4 (IMAP4) are standard messaging protocols for the Internet. The GroupWise® Internet Agent can function as a POP3 or an IMAP server, allowing access to the GroupWise domain database and message store. With POP3 or IMAP server functionality enabled, GroupWise users can download their messages from GroupWise to any POP3/IMAP4-compliant Internet e-mail client. To send messages, POP3/IMAP4 clients can identify the Internet Agent as their SMTP server.

Complete the instructions in the following sections to set up POP3/IMAP4 service:

- "Enabling POP3/IMAP4 Services" on page 684
- "Configuring Post Office Links" on page 685
- "Giving POP3 or IMAP4 Access Rights to Users" on page 686
- "Setting Up an E-Mail Client for POP3/IMAP4 Services" on page 686

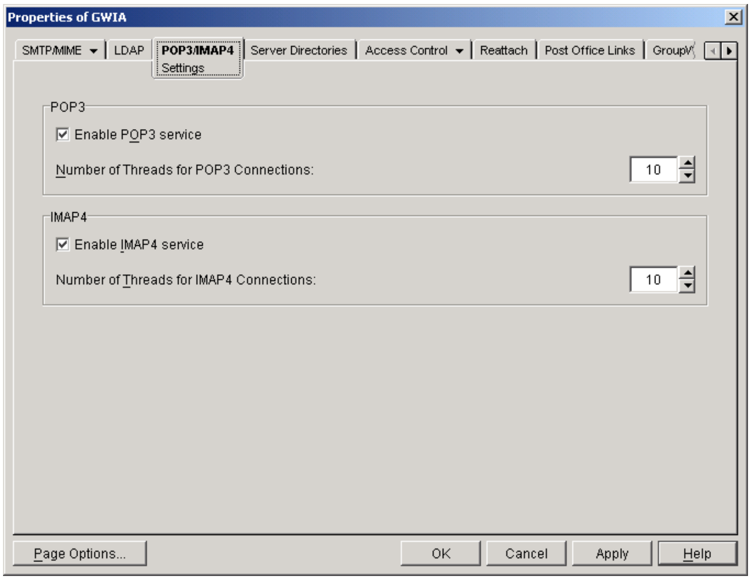
NOTE: Internal IMAP clients can connect directly to the POA, rather than connecting through the Internet Agent, as described in "Supporting IMAP Clients" on page 450. Direct connection provides faster access for internal IMAP clients.

Enabling POP3/IMAP4 Services

By default, POP3 service and IMAP 4 service are enabled. To verify that the services are enabled and configured appropriately:

1 In ConsoleOne®, right-click the Internet Agent object, then click Properties.

2 Click POP3/IMAP4 > Settings to display the POP3/IMAP 4 Settings page.



POP3

☑ Enable POP3 service

Number of Threads for POP3 Connections: 10

IMAP4

☑ Enable IMAP4 service

Number of Threads for IMAP4 Connections: 10

3. Fill in the fields:

   Enable POP3 Service: POP3 service is on by default. This setting allows POP3 downloads from a GroupWise mailbox. It corresponds with the Internet Agent's /pop3 switch.

   Number of Threads for POP3 Connections: The POP3 threads setting lets you specify the number of connections for POP3 download requests. The default is 10 threads. This setting corresponds with the Internet Agent's /pt switch.

   Enable IMAP4 Service: IMAP4 service is on by default. This setting allows IMAP4 downloads and management of GroupWise messages. It corresponds with the Internet Agent's /imap4

   Number of Threads for IMAP4 Connections: The IMAP4 threads setting lets you specify the number of connections for IMAP4 requests. The default is 10 threads. This setting corresponds with the Internet Agent's /it switch.

4. Click OK to save the changes.

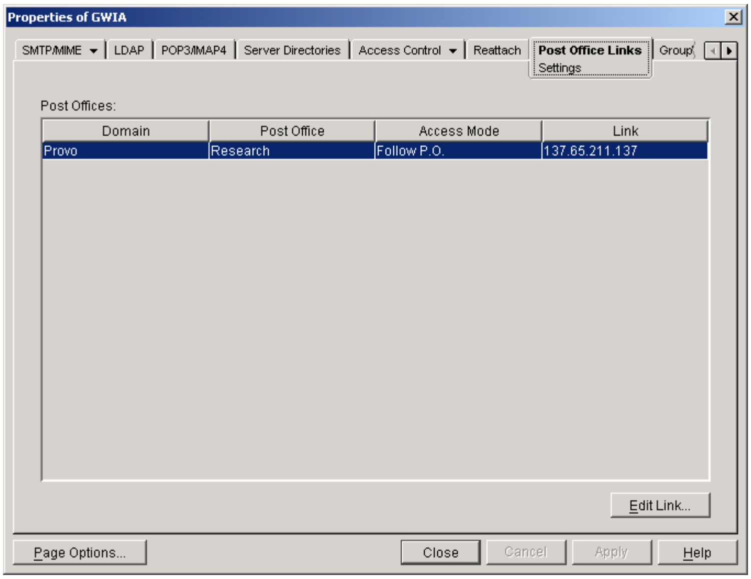
Configuring Post Office Links

To function as a POP3/IMAP4 server, the Internet Agent requires access to each post office that contains mailboxes that will be accessed by a POP3/IMAP4 client. The Internet Agent can connect directly to the post office directory through a UNC path or mapped drive, or it can use a TCP/IP connection to the Post Office Agent (POA). By default, the Internet Agent will use the access mode that has been defined for the post office (Post Office object > GroupWise tab > Post Office Settings page). If necessary, you can change the way the Internet Agent links to a post office.

To change a post office link:

1. In ConsoleOne, right-click the Internet Agent object, then click Properties.
2. Click Post Office Links > Settings.

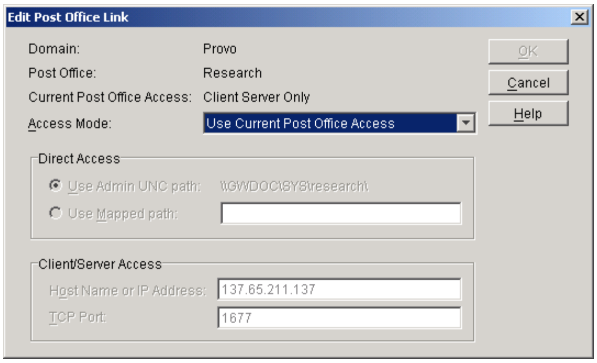
   The Post Office list displays all post offices in your GroupWise system and how the Internet Agent connects to them



Post Offices:

Domain	Post Office	Access Mode	Link
Provo	Research	Follow P.O.	137.65.211.137

3. In the Post Offices list, select the post office whose link information you want to change, then click Edit Link to display the Edit Post Office Link dialog box.



Domain: Provo

Post Office: Research

Current Post Office Access: Client Server Only

Access Mode: Use Current Post Office Access

Direct Access

● Use Admin UNC path: \\GWDOC\SYS\research\

○ Use Mapped path:

Client/Server Access

Host Name or IP Address: 137.65.211.137

TCP Port: 1677

4 Define the following properties:

Access Mode: The access mode determines whether the Internet Agent will use client/server access, direct access, or both client/server and direct access to connect to the post office. With client/server and direct, the Internet Agent first tries client/server access; if client/server access fails, it then tries direct access. You can also choose to use the same access mode currently defined for the post office (on the Post Office object's Post Office Settings page). The current access mode is displayed in the Current Post Office Access field.

Direct Access: When connecting to the post office in direct mode, the Internet Agent can use the post office's UNC path (as defined on the Post Office object's Identification page) or a mapped path that you enter.

Client/Server Access: When connecting to the post office in client/server mode, the Internet Agent must know the hostname (or IP address) and port number of the Post Office Agent running against the post office.

5 Click OK.

6 Repeat Step 3 through Step 5 for each post office whose link you want to change.

Giving POP3 or IMAP4 Access Rights to Users

Access to POP3/IMAP4 services is determined by the class of service in which they are a member. By default, all users are members of the default class of service, which gives them POP3 and IMAP4 access.

If you have changed the default class of service to exclude POP3 or IMAP4 access rights, or if you've defined additional classes of services that do not provide POP3 or IMAP4 access rights, you might want to evaluate your currently defined classes of service to ensure that they provide the appropriate POP3 or IMAP4 access. For details, see Chapter 49, "Controlling User Access," on page 705.

Setting Up an E-Mail Client for POP3/IMAP4 Services

With the Internet Agent set up as a POP3 and/or IMAP4 server, you can configure users' e-mail clients to download messages from GroupWise mailboxes.

Most e-mail clients are configured differently. However, all Internet clients will need to know the following information:

- **POP3/IMAP4 Server:** This is the DNS hostname or IP address of the Internet Agent.
- **Login Name:** This is the user's GroupWise user ID. For POP3 clients, there are several user ID login options you can use to control how the Internet Agent handles the user's messages.

For example, you can limit how many messages are downloaded each session. For more information, see "User ID Login Options" on page 687.

- **Password:** This is the user's existing GroupWise mailbox password. POP3/IMAP4 services requires users to have passwords assigned to their mailboxes.

User ID Login Options

With POP3 clients, users can add the options listed in the table below to the login name (GroupWise user ID) to control management of their mailbox messages. If used, these options override the POP3 settings assigned through the user's class of service (see "Creating a Class of Service" on page 706).

Login options are appended to the user ID name with a colon character (:) between the user ID name and the switches:

Syntax: *user_ID:switch*

Example: `User1:v=1`

You can combine options by stringing them together after the user ID and the colon without any spaces between the options:

Syntax: *user_ID:switch1switch2*

Example: `User1:v=1sdl=10`

The syntax for the user ID options is not case sensitive. Please note that login options are not required. If you do not want to include any login options, just enter the user ID name in the text box, or following the USER command if you are using a Telnet application as your POP3 client.

Option	Explanation	Example
v=*number between 1-31*	The v option defines the POP3 client's view number. If multiple POP3 clients access the same GroupWise mailbox, each client must use a different view number in order to see a fresh mailbox. For example, if two POP3 clients access a mailbox and the first client downloads the unread messages, the second client will not be able to download the messages unless it is using a different view number than the first client. If this option is not used, the default value is 1.	*User_ID*:v=1
d	The d option deletes the messages from the GroupWise mailbox after they have been downloaded to the POP3 client.	*User_ID*:d
p	The p option purges the messages from the GroupWise mailbox after they have been downloaded to the POP3 client.	*User_ID*:p
t=*1-1000*	The t option defines the download period, starting with the current day. For example, if you specify 14, then only messages that are 14 days old or newer will be downloaded. If this option is not used, the default value is 30 days.	*User_ID*:t=14

Option	Explanation	Example
n	The n option downloads messages in RFC-822 format rather than the default MIME format.	`User_ID:N`
m	The m option downloads messages in MIME format. This is the default.	`User_ID:M`
s	The s option presets the file size when the STAT command is executed. If the users' mailbox contains a lot of messages or large messages, it can take a long time to calculate the file size. With this option, the STAT command will always report an artificial file size of 1, which can save time.	`User_ID:S`
l=*1-1000*	The l option limits the number of messages to download for each POP3 session. For example, if you want to limit the number of messages to 10, you would enter l=10. If this option is not used, the default value is 100 messages.	`User_ID:L=10`

Configuring Paging Services

The GroupWise® Internet Agent includes the ability to send a GroupWise message to a pager through an Internet paging service provider. The Internet Agent's paging service includes the following features:

- **Smart forwarding:** If a message has been replied to or forwarded before being sent to a pager, the Internet Agent identifies the original message and sends it only.
- **Easy to read originator information:** The Internet Agent sends the original From, Subject, and Message information to the pager, rather than cryptic Header information.
- **User block control:** By using the /l=*length* and /b=*number* switches on the message's To line, the sender can control the block length and number of blocks to send to the pager. By default, the Internet Agent sends 255 bytes per block (/l=255 /b=1).

To set up and use paging services, complete the tasks in the following sections:

- "Setting Up Paging" on page 688
- "Using Paging" on page 689

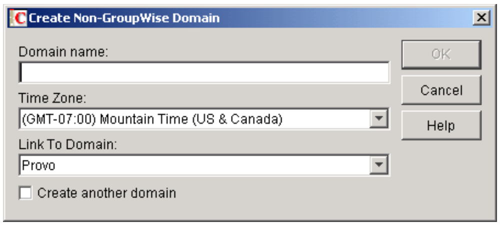
Setting Up Paging

To set up the Internet Agent's paging service, you need to create a non-GroupWise domain to represent the paging service and then use your Internet Agent to link your system to the non-GroupWise domain. The non-GroupWise domain enables GroupWise to correctly identify pager messages and route messages to the Internet Agent, which can then send the messages to the Internet.

- "Creating a Non-GroupWise Domain" on page 688
- "Linking the Internet Agent to the Non-GroupWise Domain" on page 689

Creating a Non-GroupWise Domain

1 In ConsoleOne®, right-click the GroupWise System object, click New, then click Non-GroupWise Domain to display the Create Non-GroupWise Domain dialog box.



Domain name:

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Link To Domain: Provo

□ Create another domain

2. Fill in the following information:

   Domain Name: Provide the domain with a name such as Page. Users will need to know the name when addressing pager messages.

   Time Zone: Select the time zone in which the Internet Agent is located.

   Link to Domain: Select the domain in which the Internet Agent is located.

3. Click OK to create the domain.

Linking the Internet Agent to the Non-GroupWise Domain

1. In ConsoleOne, click the Tools menu > GroupWise Utilities > Link Configuration to display the GroupWise Link Configuration tool.
2. In the drop-down list, select the domain that owns the Internet Agent that you are using for this paging service.
3. In the Outbound Links box, right-click the non-GroupWise domain, then click Edit to display the Edit Domain Link dialog box.
4. Click Yes to accept the domain path as the mapped path and display the Edit Domain Link dialog box.
5. In the Link Type field, select Gateway.
6. In the Gateway Link field, select the Internet Agent.
7. In the Gateway Access String field, type **`-page`**.
8. Click OK to save the information.
9. Click the File menu > Exit > Yes to save your changes and exit the Link Configuration tool.
10. Restart the Internet Agent.

Using Paging

To use paging, GroupWise users must address messages to the non-GroupWise domain, specifying the PIN number of the pager and the hostname of the paging service in the following format:

`domain:pin@paging_service_provider`

For example,

```
page:123456789@skytel.com
```

```
page:123456789@epage.arch.com
```

By using the /l=*length* and /b=*number* switches on the message's To line, the sender can control the block length and number of blocks to send to the pager. For example,

```
page:123456789@epage.arch.com/l=128/b=4
```

By default, the Internet Agent sends 255 bytes per block (/l=255/b=1).

48 Configuring Simplified Addressing

How outbound and inbound messages need to be addressed for your GroupWise® system to properly deliver them depends largely on how you configure your GroupWise system.

The following sections show the basic addressing syntax required if you don't configure your GroupWise system for simplified addressing and provide instructions for configuring your system for simplified addressing.

- "Basic Addressing Syntax" on page 691
- "Simplifying Addressing" on page 692

Basic Addressing Syntax

The following sections provide information about the address syntax required for GroupWise users to send and receive Internet messages.

- "Sending Messages" on page 691
- "Receiving Messages" on page 692
- "Receiving Replies to Sent Messages" on page 692

The syntax assumes that you have not configured your GroupWise system to simplify addressing. If, after reviewing the information below, you decide that you want to simplify addressing, you have the following options:

- Enable your GroupWise system to use an Internet-style address format (*user@host*) rather than the standard GroupWise address format (*user_ID.post_office.domain*). This is the recommended configuration. For details, see Chapter , "Internet-Style Addressing," on page 87.
- Add specific Internet sites (hostnames) and/or Internet users to your GroupWise system, or define addressing rules that enable the GroupWise system to recognize Internet-style addresses and route them to the Internet Agent. This can require much work on your part and is not the recommended configuration. For details, see "Simplifying Addressing" on page 692.

Sending Messages

GroupWise users can send Internet messages using the following syntax:

```
internet_agent:"user@host"
```

For example:

```
gwia:"rcollins@novell.com"
```

This addressing syntax requires you to provide GroupWise users with the name of the Internet Agent (in this example, gwia). Users must also place quotation marks around the *user@host* portion of the address.

Receiving Messages

For a GroupWise user to receive an Internet message, the message address must include the GroupWise addressing elements (*user_ID.post_office.domain*) that will make the address unique within the GroupWise system.

UserID is Unique: If a GroupWise user ID is unique within your GroupWise system, the user's Internet address can include only the user ID (*user_ID@host*). For example, jsmith@novell.com.

Post Office is Unique: If the GroupWise user ID does not create a unique address, the address must also include the user's post office (*user_ID.post_office@host*). For example, jsmith.research@novell.com.

Domain is Unique: If the GroupWise user ID and post office do not create a unique address, the address must also include the user's domain (*user_ID.post_office.domain@host*). For example, jsmith.research.provo@novell.com.

Receiving Replies to Sent Messages

When sending messages, the Internet Agent automatically adds the addressing elements necessary for the user's address to be unique in your GroupWise system.This ensures that the message's From line contains the address required to send a message back to the GroupWise user.

You can also specify the exact elements (*user_ID*, *user_ID.post_office* or *user_ID.post_office.domain*) that will be included in the address. How you do so depends on whether or not your GroupWise system is configured for Internet-style addressing:

- **Internet-style addressing enabled:** The user's address is determined by the preferred address format assigned to him or her. For information, see "Enabling Internet Addressing" on page 92.
- **Internet-style addressing disabled:** The Sender's Address Format field (Internet Agent object > GroupWise tab > Address Handling page > Sender's Address Format) determines the address format. For more information, see "Configuring How the Internet Agent Handles E-Mail Addresses" on page 664. The /aql startup switch can also be used for this same purpose.

Simplifying Addressing

The recommended way to simplify addressing is to enable your GroupWise system to use Internet-style addressing as its primary addressing format rather than the standard GroupWise addressing format. For information about enabling Internet-style addressing, see Chapter , "Internet-Style Addressing," on page 87.

If you choose not to enable Internet-style addressing, you can complete the tasks in the following section to simplify the Internet addressing syntax. You should review each section before deciding which method you want to use.

- "Creating a Non-GroupWise Domain Structure" on page 692
- "Creating a Customized Addressing Rule" on page 700

Creating a Non-GroupWise Domain Structure

A non-GroupWise domain structure includes a GroupWise domain that represents the Internet, post offices that represent Internet sites (hosts), and users that represent users located at those Internet sites.

Defining the Internet as a non-GroupWise domain enables GroupWise users to use the following syntax to send messages to Internet users:

`domain:user@host (internet:jsmith@novell.com)`

Adding Internet sites (hosts) as post offices in the domain enables GroupWise users to use the following syntax when sending messages to users at those Internet sites:

`user@post_office (jsmith@novell)`

Adding an Internet site's users to the post office enables GroupWise users to select the users from the GroupWise Address Book or use the following syntax when sending messages to those users:

`user (jsmith)`

You can create as much of the structure as is necessary to provide the desired addressing level. The following sections provide instructions:

- "Simplifying Syntax to domain:user@host" on page 693
- "Simplifying Syntax to user@postoffice" on page 696
- "Simplifying Syntax to User" on page 699

Simplifying Syntax to *domain*:*user@host*

By performing the following tasks, you can configure your GroupWise system so that users can send Internet messages using the *domain*:*user@host* syntax.

- "Creating a Non-GroupWise Domain" on page 693
- "Linking to the Non-GroupWise Domain" on page 694

Creating a Non-GroupWise Domain

The non-GroupWise domain represents the Internet and allows GroupWise to route Internet-bound messages to the Internet Agent. If you create a domain called "internet," GroupWise users would use the following syntax to send Internet messages:

`internet:user@host`

Messages sent from GroupWise to the Internet must be converted from GroupWise format to MIME or RFC-822 format. By default, the Internet Agent converts messages to MIME format. If your GroupWise users need to send messages in both MIME format and RFC-822 format, you may want to create two non-GroupWise domains, one to handle messages that need to be sent in MIME format and one to handle messages that need to be sent in RFC-822 format.

For example, if you define the domain "mime" and configure the Internet Agent to convert all messages sent to that domain to MIME format, GroupWise users can use the following syntax to send MIME-formatted messages:

`mime:user@host`

If you define the domain "rfc822" and configure the Internet Agent to convert all messages sent to that domain to RFC-822 format, GroupWise users can use the following syntax to send RFC-822 formatted messages:

`rfc822:user@host`

To create a non-GroupWise domain:

1. In ConsoleOne®, right-click GroupWise System (in the left pane), click New, then click Non-GroupWise Domain.

2 Fill in the fields:

Domain Name: Enter a name that has not been used for another domain in your system (for example, Internet).

Time Zone: This should match the time zone for the Internet Agent. If it does not, select the correct time zone.

Link to Domain: Select the domain in which the Internet Agent is located.

3 Click OK to create the non-GroupWise domain.

The domain will appear under GroupWise System in the left pane.

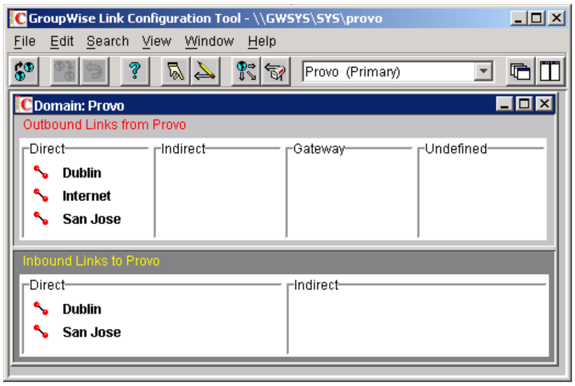
Linking to the Non-GroupWise Domain

After you have created the non-GroupWise domain, you must link the Internet Agent's domain to the non-GroupWise domain. This enables the GroupWise system to route all Internet messages to the Message Transfer Agent (MTA) located in the Internet Agent's domain. The MTA can then route the messages to the Internet Agent, which will send them to the Internet.

To link to the non-GroupWise domain:

1 In ConsoleOne, click the Tools menu > GroupWise Utilities > Link Configuration to display the Link Configuration tool.

By default, the Link Configuration tool displays the links for the domain that you are currently connected to.

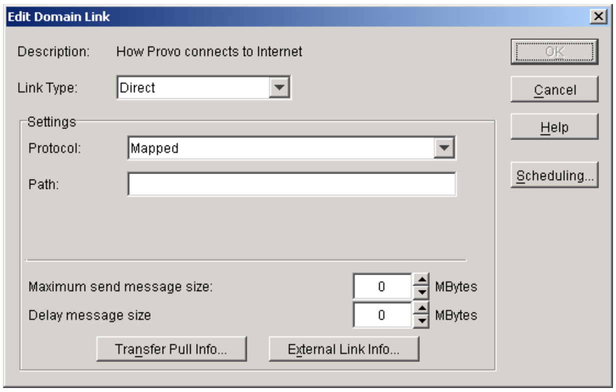


2 If the Internet Agent's domain is not the currently displayed domain, select it from the list of domains on the toolbar.

The non-GroupWise domain should be displayed in the Direct column. In the screen displayed under step 1, Internet is the non-GroupWise domain.

3 Double-click the non-GroupWise domain to display the Edit Domain Link dialog box.

NOTE: If you are prompted that the mapped path is empty, click Yes to dismiss the prompt and display the Edit Domain Link dialog box.



Description: How Provo connects to Internet

Link Type: Direct

Settings

Protocol: Mapped

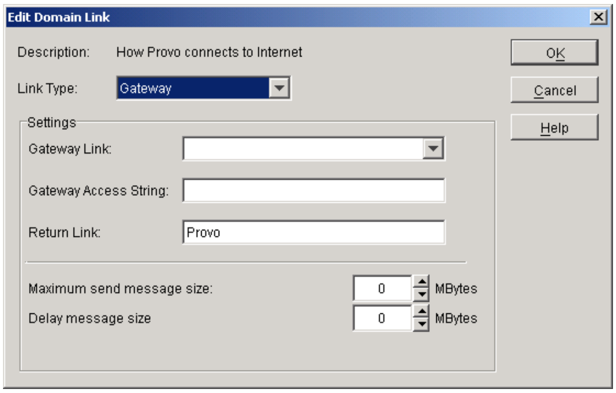
Path:

Maximum send message size: 0 MBytes

Delay message size 0 MBytes

4 In the Link Type field, select Gateway.

After you select Gateway, the dialog boxes changes to display the settings required for a gateway link.



Description: How Provo connects to Internet

Link Type: Gateway

Settings

Gateway Link:

Gateway Access String:

Return Link: Provo

Maximum send message size: 0 MBytes

Delay message size 0 MBytes

5 Fill in the following fields:

Gateway Link: Select the Internet Agent.

Gateway Access String: If you want to specify the conversion format (RFC-822 or MIME) for messages sent to the domain, include one of the following parameters: -rfc822 or -mime. If you do not use either of these parameters, the Internet Agent will convert messages to the format specified in its startup file. The default is for MIME conversion (as specified by the Internet Agent's /mime startup switch).

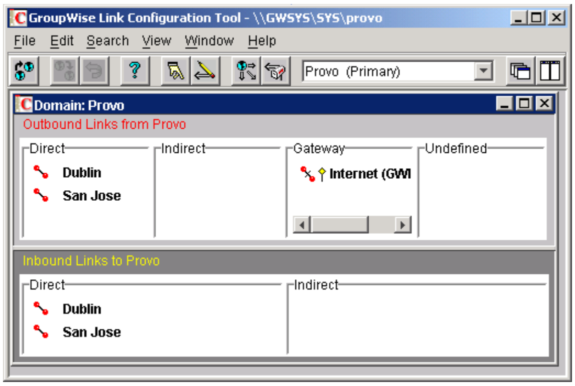
Return Link: Leave this field as is. It does not apply to the Internet Agent.

Maximum Send Message Size: If you want to limit the size of messages that the Message Transfer Agent (MTA) in the Internet Agent's domain will pass to the Internet Agent, specify the maximum size. This will be applied to all messages. If you want to limit the size of messages sent by specific users or groups of users, you can also use the Access Control feature. For details, see Chapter 49, "Controlling User Access," on page 705.

Delay Message Size: If you want the MTA to delay routing of large-sized messages to the Internet Agent, specify the message size. Any messages that exceed the message size will be assigned a lower priority by the MTA and will be processed after the higher priority messages.

6 Click OK to save the changes.

The non-GroupWise domain is moved from the Direct column to the Gateway column. For a description of the link symbols in front of the domain names, see the Help in the Link Configuration tool.



7 Click the File menu, click Exit, then click Yes to exit the Link Configuration tool and save your changes.

At this point, users can exchange e-mail with other Internet users using the syntax *domain*:*user@host*. Make sure you distribute the name of the domain to your users.

Simplifying Syntax to *user@postoffice*

This section assumes that you have already created a non-GroupWise domain. If you have not, see "Creating a Non-GroupWise Domain" on page 693.

After you've created a non-GroupWise domain to represent the Internet, you can add post offices to the domain to represent different Internet hosts. For example, if your GroupWise users frequently send messages to users at XYZ.COM, you can define XYZ.COM as a post office. GroupWise users would then use the following syntax to send messages to those users:

```
user@postoffice
```

To simplify the addressing syntax to this level, complete the following tasks:

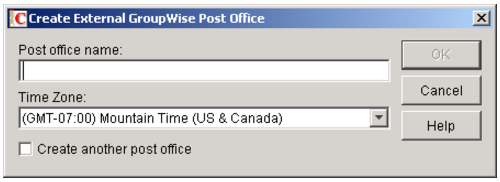
- "Creating a Post Office to Represent a Internet Host" on page 696
- "Adding the Hostname As an Alias" on page 697

Creating a Post Office to Represent a Internet Host

When creating a post office to represent an Internet host, the post office name cannot be identical to the hostname because the period that separates the hostname components (for example, novell.com) is not a valid character for post office names. GroupWise reserves the period for its addressing syntax of *user_ID.post_office.domain*. Therefore, you should choose a name that is closely related to the hostname.

To create the post office:

1 In ConsoleOne, right-click the non-GroupWise domain that represents the Internet, click New, then click External Post Office.



Create External GroupWise Post Office

Post office name:

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

□ Create another post office

2 Fill in the following fields:

Post Office Name: Enter a name that will associate the post office with the Internet host. Do not use the fully-qualified hostname.

Time Zone: Select the time zone in which the Internet host is located.

3 Click OK to create the post office.

The post office is added under the non-GroupWise domain.

Adding the Hostname As an Alias

When a GroupWise user sends a message to a user at the Internet host, he or she will use the post office name in the address:

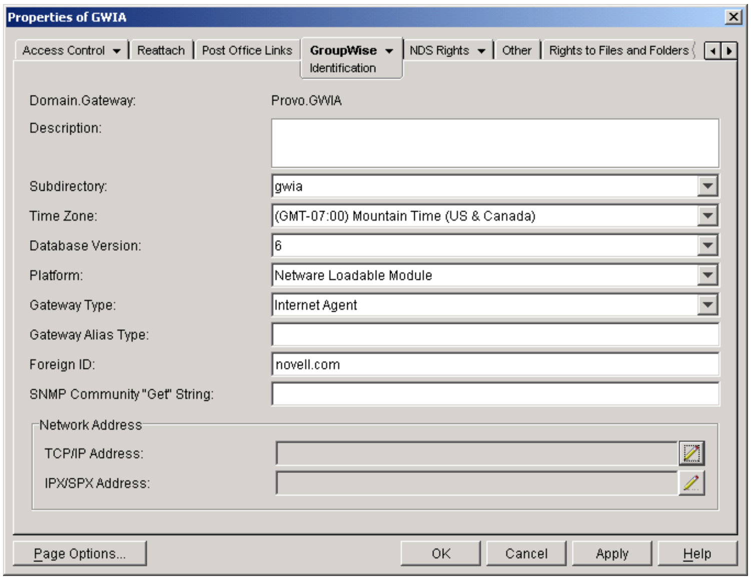
```
user@post_office
```

For the Internet Agent to send the message, you need to associate the Internet hostname with the post office. You do this by defining the hostname as an alias for the post office.

To create a post office alias:

1 In ConsoleOne, right-click the Internet Agent object, click Properties.

2 Click GroupWise > Identification to display the Identification page.



Properties of GWIA

Domain.Gateway: Provo.GWIA

Description:

Subdirectory: gwia

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Database Version: 6

Platform: Netware Loadable Module

Gateway Type: Internet Agent

Gateway Alias Type:

Foreign ID: novell.com

SNMP Community "Get" String:

Network Address

TCP/IP Address:

IPX/SPX Address:

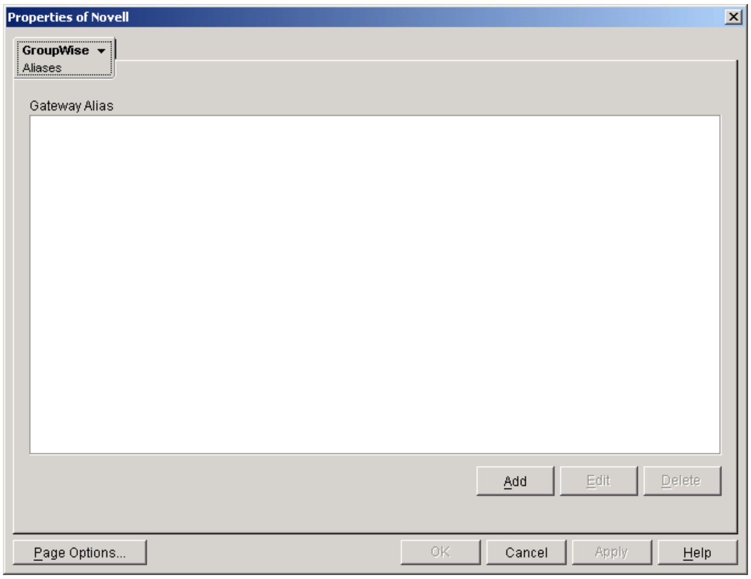
3 In the Gateway Alias Type field, enter an alias type.

This can be any name you want, including the same name as the Internet Agent. It will be used to associate the post office alias with the Internet Agent.

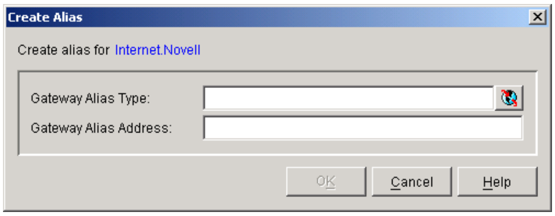
4 Click OK to save the gateway alias type information.

5 Right-click the post office you created for the Internet host, then click Properties.

6 Click GroupWise > Gateway Aliases to display the Gateway Aliases page.



7 Click Add to display the Create Alias dialog box.


Create alias for Internet.Novell

Gateway Alias Type:

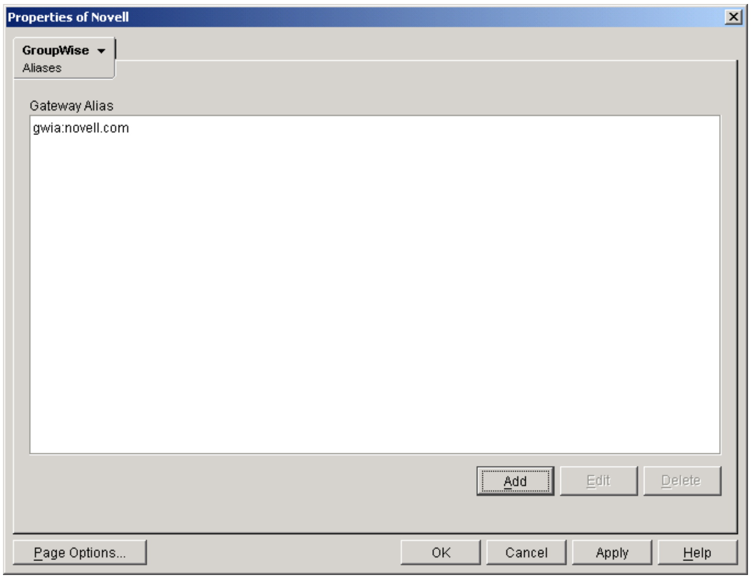
Gateway Alias Address:

8 Fill in the following fields:

Gateway Alias Type: Select the gateway alias type you assigned to the Internet Agent.

Gateway Alias: Enter the Internet hostname (for example, novell.com).

9 Click OK to add the alias to the Gateway Alias list.



Gateway Alias
gwia:novell.com

10 Click OK.

With these steps completed, GroupWise users can send a message to a user at the Internet host with the following syntax:

```
user@post_office
```

Users are not restricted to using *user@post_office* addressing. They can still use *domain*:*user@host* addressing to send messages to other users.

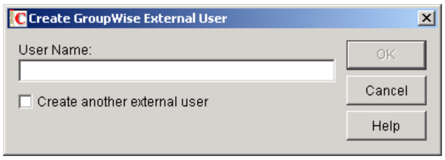
Simplifying Syntax to *User*

This section assumes that you have already completed the tasks in "Simplifying Syntax to domain:user@host" on page 693 and "Simplifying Syntax to user@postoffice" on page 696.

To configure your GroupWise system for *user* syntax, you need to add Internet users to the post offices you created to represent their Internet hosts. This not only enables the *user* syntax, but also adds the Internet users to the GroupWise Address Book.

To add an Internet user to a post office:

1 In ConsoleOne, right-click the post office that represents the user's Internet host, click New, then click External User.



User Name:

□ Create another external user

2 In the User Name field, enter the exact user portion of the user's Internet address. If the address is jsmith@novell.com, the portion you would enter is jsmith.

3 Click OK to create the external user.

4 Because the user will be displayed in the GroupWise Address Book, you might want to define the user's given name and last name. To do so, right-click the user's object, fill in the desired fields on the Identification page, then click OK to save the information.

To send a message to an Internet user who you've added, your GroupWise users can use the Address Book or enter the following syntax:

```
user
```

For example,

```
jsmith
```

User addressing does not restrict users from addressing messages to other Internet users who are not included in the GroupWise Address Book. Users can also use *domain*:*user@host* addressing, which lets them communicate with Internet users who are not yet part of your system's non-GroupWise domain structure.

Creating a Customized Addressing Rule

You can use addressing rules to determine how addresses with specific syntax elements are handled. For example, you could establish an addressing rule that enables GroupWise users to enter an Internet address (*user@host*) and then resolves it to the syntax (*internet_agent*:"*user@host*") required by the Internet Agent.

An addressing rule is not a macro; you cannot embed one rule within another rule. The addressing rule simply searches for a string pattern and replaces it with the syntax defined in the rule.

Each addressing rule you create is available for your entire GroupWise system. However, you can enable or disable a rule at the domain level.

The following sections provide information about creating and managing addressing rules:

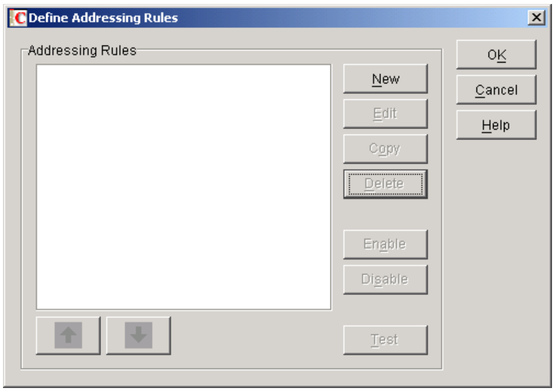
- "Creating an Addressing Rule" on page 700
- "Enabling and Disabling Addressing Rules" on page 702
- "Changing the Addressing Rule Order" on page 703

Creating an Addressing Rule

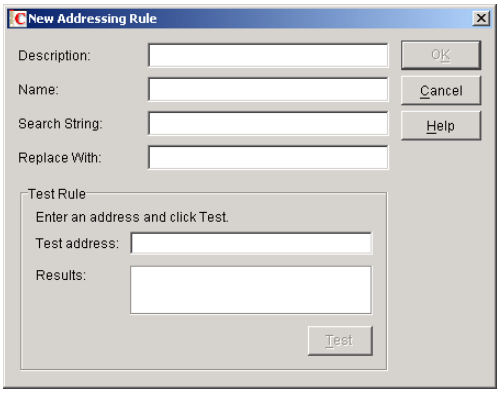
GroupWise uses *user_ID@domain.post_office* syntax internally. Because of this, it is important the addressing rule you create includes an Internet domain identifier such as .com or .edu. You may need to include Internet domain identifiers for all the Internet addresses you will use. For example, if you want to send to jsmith@novell.com, bharris@college.edu, and tsternes@marketing.net, you should create a rule for each domain identifier (.com, .edu, and .net).

To create an addressing rule:

1 In ConsoleOne, click the Tools menu > GroupWise System Operations > Addressing Rules.



2 Click New to display the New Addressing Rule dialog box.



3 Fill in the following fields:

Description: Enter a short description for the rule. The description is what appears when the rule is listed in the Addressing Rules dialog box.

Name: Enter the name you want to use for the rule (for example, Internet Addresses).

Search String: Enter a string of characters (including any wildcards for variable elements) that represents the addressing syntax you expect for an Internet message. The syntax must have at least one unique character that will identify it for your rule as an Internet address. The rule can then plug in the required, missing elements of the explicit address. For example, if you want GroupWise users to enter *user@host* when addressing Internet messages, you could define the search string as `*@*.com`.

Replace With: Enter the symbol for the variable string (information typed in by the user) that you want to replace for the wildcard characters. In addition to the variable symbol, you can also add any additional static elements required in the explicit address. A good replacement string is internet:"%1%2.com.". When the message is sent, the rule refers to the wildcards in search string order. That is, %1 (replace string 1) replaces the first wildcard in the search string, %2 replaces the second wildcard, and so on. The replacement variables do not have to be positioned in numerical order in the replacement string; instead, they must be placed in the string according to the order required for the explicit address.

For example, one of your GroupWise users sends a message using the following address: jsmith@sales.novell.com.

Address syntax (entered by user): `jsmith@sales.novell.com`

Search string: `*@*.com`

Replacement string: `internet"%1@%2.com`

Results: `internet"jsmith@sales.novell.com"`

4 Type an address in the Test Address field just as you would expect a GroupWise user to type an address in the GroupWise client.

5 Click Test to determine if your search and replace strings result in an accurately resolved explicit address.

6 Click OK to save the addressing rule.

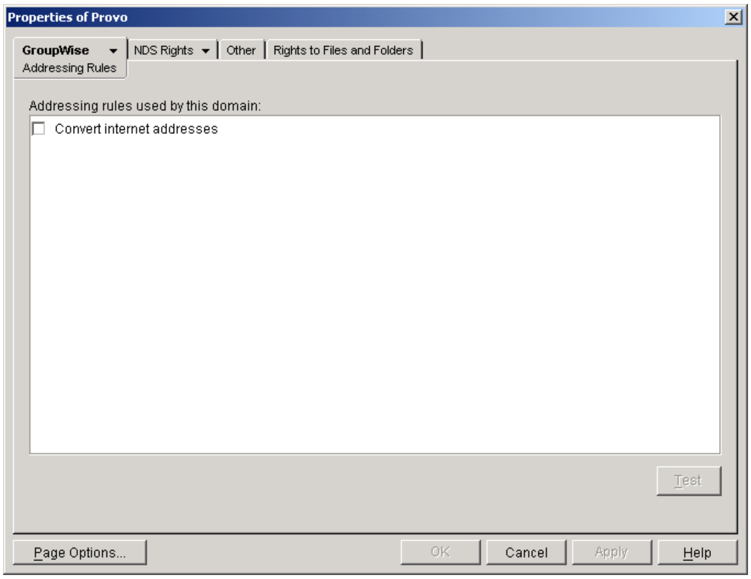
Enabling and Disabling Addressing Rules

Addressing rules are not automatically enabled. You need to enable them in each domain to which you want them applied

To enable or disable addressing rules:

1 Right-click a Domain object, then click Properties.

2 Click GroupWise > Addressing Rules to display the Addressing Rules page.

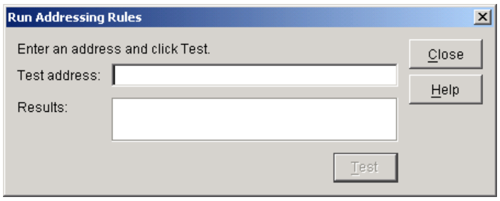


Addressing rules used by this domain:

□ Convert internet addresses

3 Click the check box to enable the addressing rule you want in this domain.

4 To ensure that the rule is being applied correctly in the domain, click Test to display the Run Addressing Rules dialog box.



Enter an address and click Test.

Test address:

Results:

5 Enter an address as if you were a user sending a message, then click Test.

The Results field displays the resolved address. If this is not the address you were expecting, check the other rules that precede the rule in the list. Addresses are evaluated against the rules in the order the rules are listed. It may be necessary to change the order of the rules (see "Changing the Addressing Rule Order" on page 703).

6. Click Close to close the Run Addressing Rule dialog box, then click OK.

Changing the Addressing Rule Order

Addressing rules are applied in the order they are encountered. If a rule is applied to an address string, the search for a rule ends.

To change the order of addressing rules:

1. In ConsoleOne, click the Tools menu > GroupWise System Operations > Addressing Rules.
2. Select a rule, then click the up-arrow to move it up in the list.

   or

   Select a rule, then click the down-arrow to move it down in the list.

49 Controlling User Access

You can use the GroupWise® Internet Agent's Access Control feature to configure a user's ability to send and receive SMTP/MIME messages to and from Internet recipients and to access his or her mailbox from POP3 or IMAP4 e-mail clients. In addition to enabling or disabling a user's access to features, you can configure specific settings for the features. For example, for outgoing SMTP/MIME messages, you can limit the size of the messages or the sites to which they can be sent.

Access Control can be implemented at a user, distribution list, post office, or domain level.

Choose from the following information to learn how to set up and use Access Control.

Classes of Service

A class of service is a specifically defined configuration of Internet Agent privileges. A class of service controls the following types of access activities:

- Whether or not SMTP/MIME messages are allowed to transfer to and from the Internet
- Whether or not SMTP/MIME messages are allowed to transfer to and from specific domains on the Internet
- The maximum size of SMTP/MIME messages that can transfer to and from the Internet
- Whether or not SMTP/MIME messages generated by GroupWise rules are allowed to transfer to the Internet
- Whether or not IMAP4 clients are allowed to access the GroupWise system
- Whether or not POP3 clients are allowed to access the GroupWise system, and if allowed, how messages to and from POP3 clients are managed by the GroupWise system

The default class of service, which all users belong to, allows incoming and outgoing SMTP/MIME messages, and allows POP3 and IMAP4 access. You can control user access, at an individual, distribution list, post office, or domain level, by creating different classes of service and adding the appropriate members to the classes. For example, you could create a class of service that would limit the size of SMTP/MIME messages for a selected individual, distribution list, post office, or domain.

Because you can assign membership at the user, distribution list, post office, and domain level, it is possible that a single user can be a member of multiple classes of service. This conflict is resolved hierarchically, as shown in the following table.

Membership assigned to a user through a...	Overrides membership assigned to the user through the...
domain	◆ default class of service
post office	◆ default class of service ◆ domain
distribution list	◆ default class of service ◆ domain ◆ post office
user	◆ default class of service ◆ domain ◆ post office

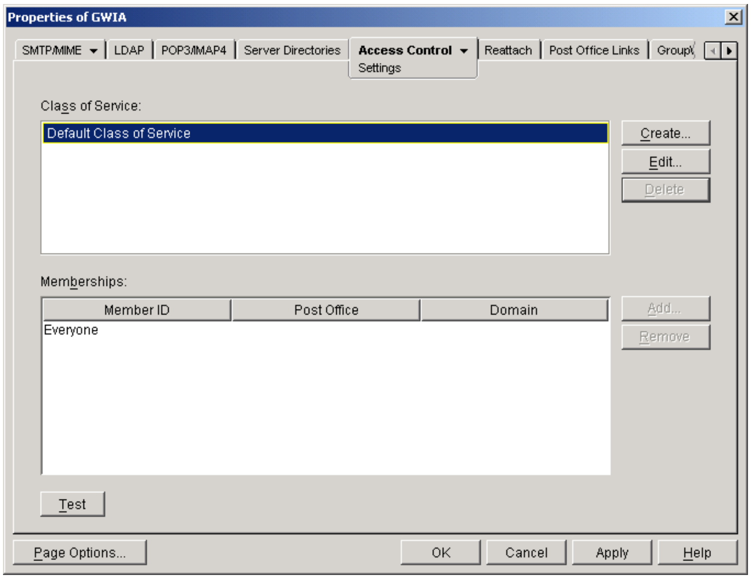
If a user's membership in two classes of service is based upon the same level of membership (for example, both through individual user membership), the class that applies is the one that allows the most privileges.

IMPORTANT: The Internet Agent uses the message size limit set for the default class of service as the maximum incoming message size for your GroupWise system. Therefore, you should set the message size for the default class of service to accommodate the largest message that you want to allow into your GroupWise system. As needed, you can then create other classes of service with smaller message size limits to restrict the size of incoming messages for selected users, distribution lists, post offices, or domain. Methods for restricting message size inside your GroupWise system are described in "Restricting the Size of Messages That Users Can Send" on page 175.

Creating a Class of Service

1 In ConsoleOne®, right-click the Internet Agent object, then click Properties.

2 Click Access Control > Settings to display the Access Control Settings page.



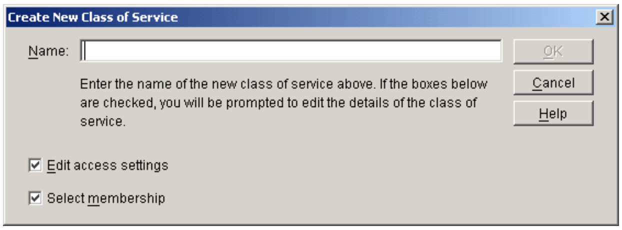
Class of Service:

Default Class of Service

Memberships:

Member ID	Post Office	Domain
Everyone		

3 Click Create to display the Create New Class of Service dialog box.



Create New Class of Service

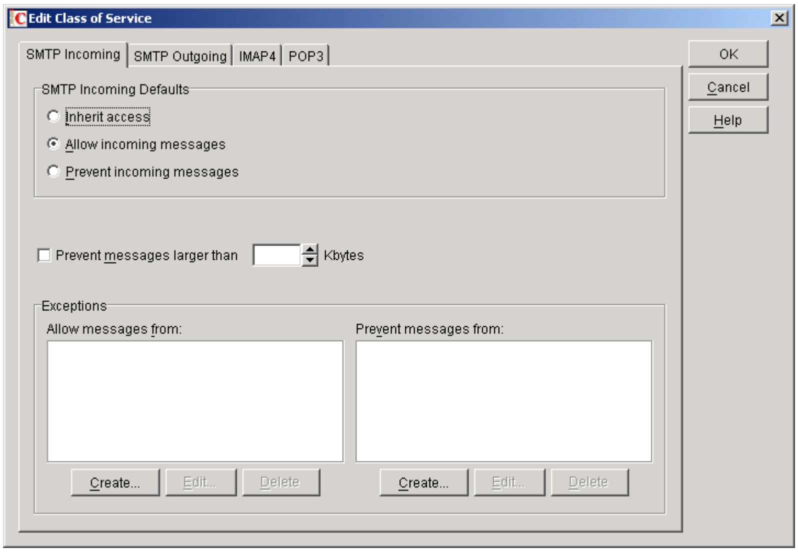
Name:

Enter the name of the new class of service above. If the boxes below are checked, you will be prompted to edit the details of the class of service.

☑ Edit access settings

☑ Select membership

4 Type a name for the class, then click OK to display the Edit Class of Service dialog box.



Edit Class of Service

SMTP Incoming Defaults

○ Inherit access

● Allow incoming messages

○ Prevent incoming messages

□ Prevent messages larger than Kbytes

Exceptions

Allow messages from:

Prevent messages from:

5 On the SMTP Incoming tab, choose from the following options:

Inherit Access: Select this option if you want members of this class of service to inherit their SMTP Incoming access from a class of service assigned at a higher level. For example, a post office would inherit the domain’s access. If the domain was not a member of a class of service, the post office would inherit the default class of service.

Allow Incoming Messages: Select this option to allow members of the class of service to receive e-mail messages through the Internet Agent. You can use the Exceptions option to prevent messages from specific Internet sites.

Prevent Incoming Messages: Select this option to prevent e-mail messages coming from the Internet. You can use the Exceptions option to allow messages from specific Internet sites.

Prevent Messages Larger Than: This option is available only if you chose Allow Incoming Messages or Prevent Incoming Messages. In the case of Prevent Incoming Messages, this option only applies to messages received from Internet sites listed in the Allow Message From list.

If you want to set a size limit on incoming messages, select the limit.

Exceptions: This option is available only if you chose Allow Incoming Messages or Prevent Incoming Messages.

Prevent Messages From: If you’ve chosen to allow incoming messages but you want to prevent messages from specific Internet sites (IP addresses or DNS hostnames), add the sites to the Prevent Messages From list.

Allow Messages From: Conversely, if you've chosen to prevent incoming messages but you want to allow messages from specific Internet sites (IP addresses or DNS hostnames), add the sites to the Allow Messages From list.

If you want to allow messages where the username is blank, add Blank-Sender-User-ID to the Allow Message From list.

6 Click the SMTP Outgoing tab, then choose from the following options:

Inherit Access: Select this option if you want members of this class of service to inherit their SMTP Outgoing access from a class of service assigned at a higher level. For example, a post office would inherit the domain's access. If the domain was not a member of a class of service, the post office would inherit the default class of service.

Allow Outgoing Messages: Select this option to allow members of the class of service to send e-mail messages over the Internet. You can use the Exceptions option to prevent messages from being sent to specific Internet sites.

Prevent Outgoing Messages: Select this option to prevent members of the class of service from sending e-mail messages over the Internet. You can use the Exceptions option to allow messages to be sent to specific Internet sites.

Prevent Messages Larger Than: This option is available only if you chose Allow Outgoing Messages or Prevent Outgoing Messages.

If you want to set a size limit on outgoing messages, specify the limit.

If a user tries to send an Internet message that exceeds the specified size, the sender receives an e-mail message indicating that the message is undeliverable and including the following explanation:

```
Message exceeds maximum allowed size
```

Allow Rule-Generated Messages: This option is available only if you chose Allow Outgoing Messages or Prevent Outgoing Messages.

Turn on this option to allow the Internet Agent to send messages that were generated by a GroupWise rule.

Exceptions: This option is available only if you chose Allow Outgoing Messages or Prevent Outgoing Messages.

If you've chosen to allow outgoing messages but you want to prevent messages from being sent to specific Internet sites (IP addresses or DNS hostnames), add the sites to the Prevent Messages To list.

Conversely, if you've chosen to prevent outgoing messages but you want to allow messages to be sent to specific Internet sites (IP addresses or DNS hostnames), add the sites to the Allow Messages To list.

7 Click the IMAP4 tab, then choose from the following options:

Inherit Access: Select this option if you want members of this class of service to inherit their IMAP4 access from a class of service assigned at a higher level. For example, a post office would inherit the domain's access. If the domain was not a member of a class of service, the post office would inherit the default class of service.

Allow Access: Select this option to allow members of the class to send and receive messages with an IMAP4 client.

Prevent Access: Select this option to prevent members of the class from sending and receiving messages with an IMAP4 client.

8 Click the POP3 tab, then choose from the following options:

Inherit Access: Select this option if you want members of this class of service to inherit their POP3 access from a class of service assigned at a higher level. For example, a post office would inherit the domain's access. If the domain was not a member of a class of service, the post office would inherit the default class of service.

Allow Access: Select this option to allow members of the class to download their GroupWise messages to a POP3 client.

Prevent Access: Select this option to prevent downloading GroupWise messages to a POP3 client.

Delete Messages from GroupWise Mailbox after Download: This option applies only if you've selected Allow Access.

If you turn on this option, messages downloaded from a GroupWise Mailbox to a POP3 client will be moved to the Trash folder in the GroupWise Mailbox.

POP3 client users can enable this option by using the *userID*:d login option when initiating their POP session. For more information, see "User ID Login Options" on page 687.

Purge Messages from GroupWise Mailbox after Download: This option applies only if you've selected Allow Access.

If you turn on this option, messages downloaded from a GroupWise Mailbox will be moved to the Mailbox's Trash folder and then emptied, completely removing the messages from the Mailbox.

POP3 client users can enable this option by using the *userID*:p login option when initiating their POP session. For more information, see "User ID Login Options" on page 687.

Convert Messages to MIME Format When Downloading: This option applies only if you've selected Allow Access.

If you turn on this option, messages downloaded to a POP3 client will be converted to the MIME format.

POP3 client users can enable this option by using the *userID*:m login option when initiating their POP session. The can disable it by using the *userID*:n login option; this converts messages to RFC-822 format. For more information, see "User ID Login Options" on page 687.

High Performance on File Size Calculations: This option applies only if you've selected Allow Access.

POP3 clients calculate the size of each message file before downloading it. Turn on this option if you want to assign a size of 1KB to each message file. This eliminates the time associated with calculating a file's actual size.

POP3 client users can enable this option by using the *userID*:s login option when initiating their POP session. For more information, see "User ID Login Options" on page 687.

Number of Days Prior to Today to Get Messages From: This option applies only if you've selected Allow Access.

Select the number of days to go back to look for GroupWise Mailbox messages to download to the POP3 client. The default is 30 days.

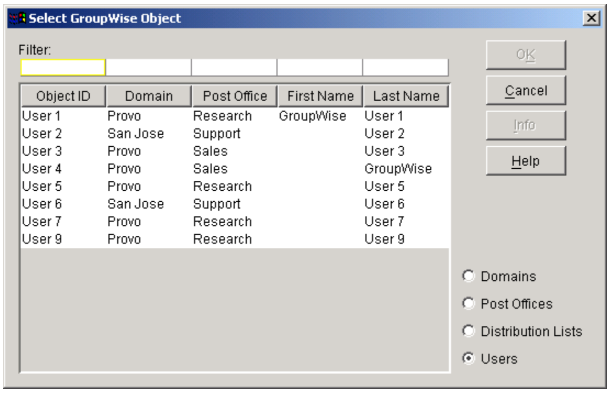
POP3 client users can override this option by using the *userID*:t=*x* login option when initiating their POP session. For more information, see "User ID Login Options" on page 687.

Maximum Number of Messages to Download: This option applies only if you've selected Allow Access.

Select the maximum number of messages a user can download at one time from a GroupWise Mailbox to a POP3 client. The default is 100 messages.

POP3 client users can override this option by using the *userID*:l=*x* login option when initiating their POP session. For more information, see "User ID Login Options" on page 687.

9 Click OK to display the Select GroupWise Object dialog box.

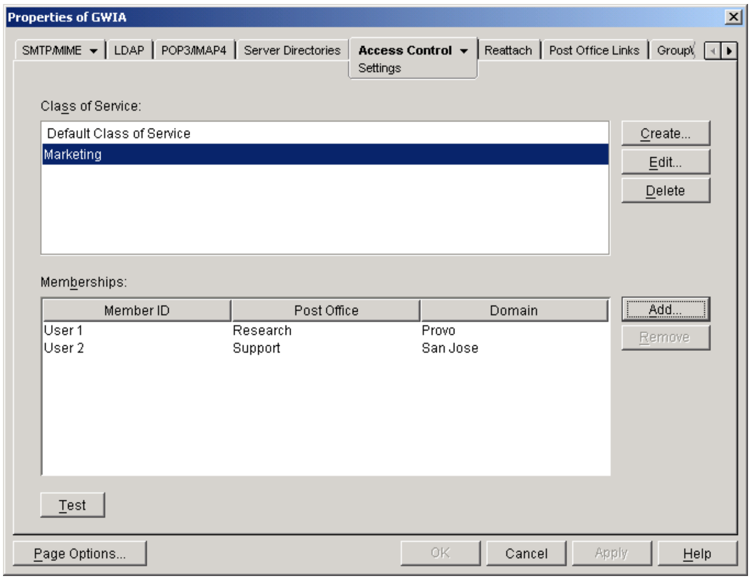


Object ID	Domain	Post Office	First Name	Last Name
User 1	Provo	Research	GroupWise	User 1
User 2	San Jose	Support		User 2
User 3	Provo	Sales		User 3
User 4	Provo	Sales		GroupWise
User 5	Provo	Research		User 5
User 6	San Jose	Support		User 6
User 7	Provo	Research		User 7
User 9	Provo	Research		User 9

○ Domains
○ Post Offices
○ Distribution Lists
● Users

10 Click Domains, Post Offices, Distribution Lists, or Users to display the list you want.

11 In the list, select the domain, post office, distribution list, or user you want, then click Add to add the object as a member in the class. You can Control+click or Shift+click to select multiple users.



Class of Service:

Default Class of Service
Marketing

Memberships:

Member ID	Post Office	Domain
User 1	Research	Provo
User 2	Support	San Jose

12 To add additional domains, post offices, distribution lists or users as members of the class of service, select the class of server, then click Add to display the Select GroupWise Object dialog box.

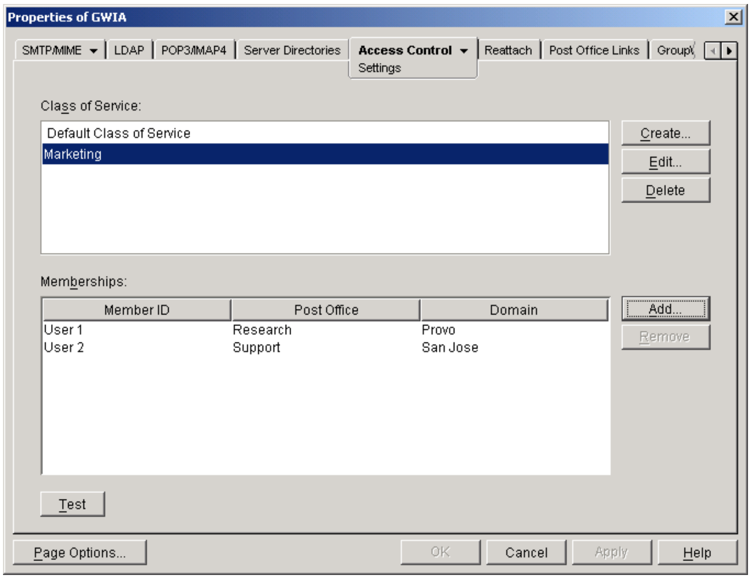
13 Click OK (on the Settings page) when finished adding members.

Testing Access Control Settings

If you've created multiple classes of service, you might not know exactly which settings are being applied to a specific object (domain, post office, distribution list, or user) and which class of service the setting is coming from. To discover an object's settings, you can test the object's access.

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click Access Control > Settings to display the Access Control Settings page.



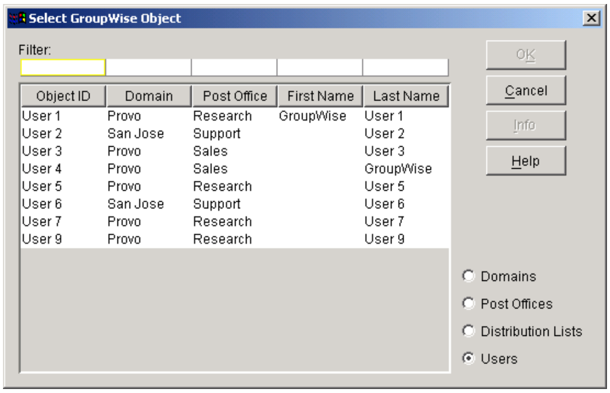
Class of Service:

- Default Class of Service
- Marketing

Memberships:

Member ID	Post Office	Domain
User 1	Research	Provo
User 2	Support	San Jose

3 Click Test to display the Select GroupWise Object dialog box.



Object ID	Domain	Post Office	First Name	Last Name
User 1	Provo	Research	GroupWise	User 1
User 2	San Jose	Support		User 2
User 3	Provo	Sales		User 3
User 4	Provo	Sales		GroupWise
User 5	Provo	Research		User 5
User 6	San Jose	Support		User 6
User 7	Provo	Research		User 7
User 9	Provo	Research		User 9

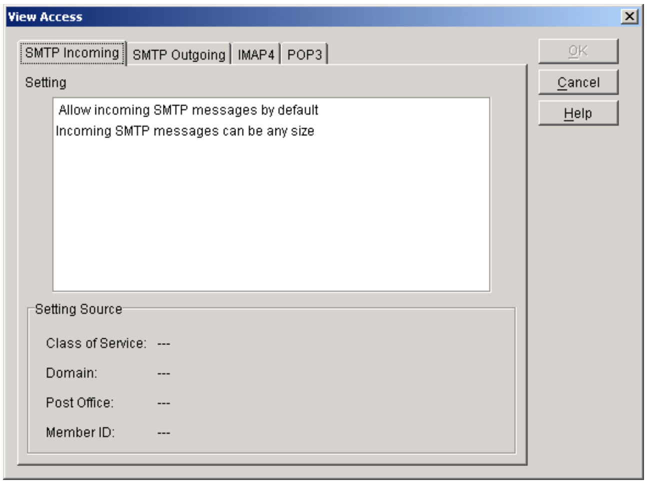
○ Domains
○ Post Offices
○ Distribution Lists
● Users

You use this dialog box to select the object (domain, post office, distribution list, or user) whose access you want to test.

4 Click Domains, Post Offices, Distribution Lists, or Users to display the list you want. For example, if you want to see what access an individual user has, click Users.

5 In the list, select the object you want to view, then click View Access.

The tabbed pages show the access control settings for SMTP Incoming, SMTP Outgoing, IMAP4, and POP3 as they are applied to that user, distribution list, post office, or domain.



Setting

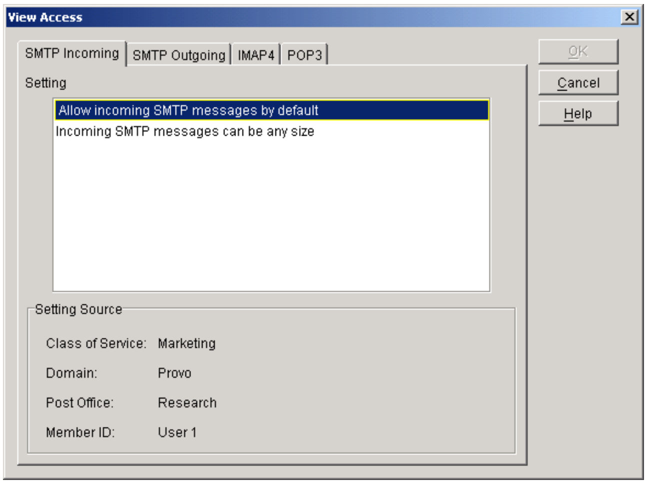
Allow incoming SMTP messages by default
Incoming SMTP messages can be any size

Setting Source

Class of Service: ---
Domain: ---
Post Office: ---
Member ID: ---

6 To view the source for a specific setting, select the setting in the Setting box

The Setting Source fields display the class of service being applied to the object. It also displays the Member ID through which the class is being applied.



Setting

Allow incoming SMTP messages by default
Incoming SMTP messages can be any size

Setting Source

Class of Service: Marketing
Domain: Provo
Post Office: Research
Member ID: User 1

7 When finished, click OK.

Maintaining the Access Control Database

The Access Control database stores the information for the various classes of service you have created. If any problems occur with a class of service, you can validate the database to check for errors with the records and indexes contained in the database. If errors are found, you can recover the database.

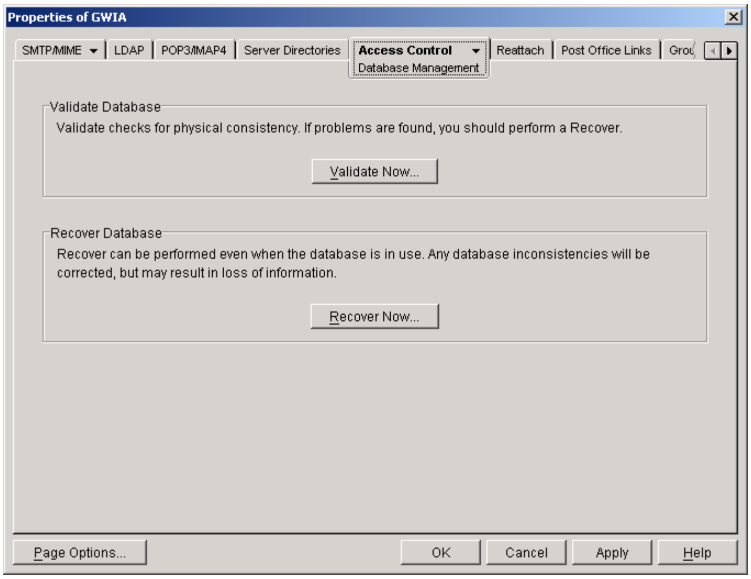
The Access database, gwac.db, is located in the *domain*\wpgate\gwia directory.

- "Validating the Database" on page 713
- "Recovering the Database" on page 713

Validating the Database

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click Access Control > Database Management to display the Database Management page.



Properties of GWIA

Validate Database

Validate checks for physical consistency. If problems are found, you should perform a Recover.

Recover Database

Recover can be performed even when the database is in use. Any database inconsistencies will be corrected, but may result in loss of information.

3 Click Validate Now.

4 After the database has been validated, click OK.

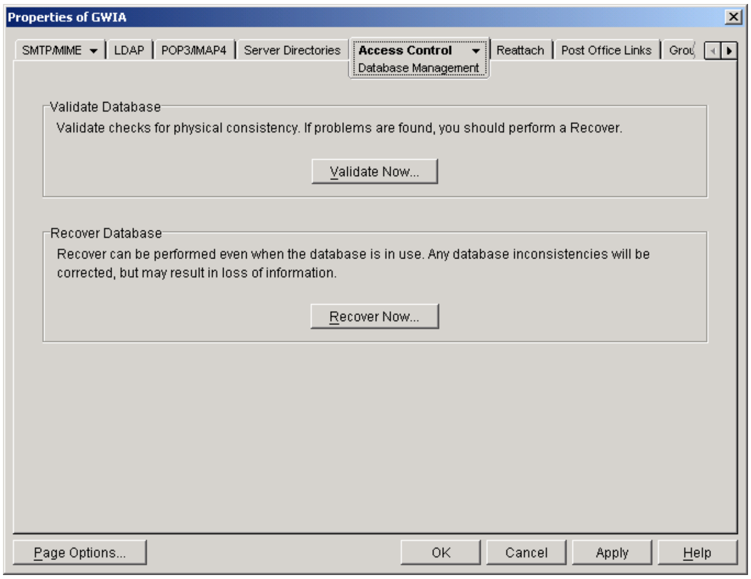
5 If errors were found, see Recovering the Database below.

Recovering the Database

If you encountered errors when validating the database, you must recover the database. During the recovery process a new database is created and all intact records are copied to the new database. Some records might not be intact, so you should check the classes of services to see if any information was lost.

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click Access Control > Database Management to display the Database Management page.



Validate checks for physical consistency. If problems are found, you should perform a Recover.

Recover can be performed even when the database is in use. Any database inconsistencies will be corrected, but may result in loss of information.

3 Click Recover Now.

4 Click OK.

5 Check your class of service list to make sure that it is complete.

50 Setting Up Accounting

The Internet Agent can supply accounting information for all messages, including information such as the message's source, priority, size, and destination.

The accounting file is an ASCII-delimited text file that records the source, priority, message type, destination, and other information about each message sent through the gateway. The file, which is updated daily at midnight (and each time the Internet Agent restarts, is called acct and is located in the *xxx*.prc directory. If no accountant is specified for the gateway in ConsoleOne®, the file is deleted and re-created each day. Follow the steps below to set up accounting.

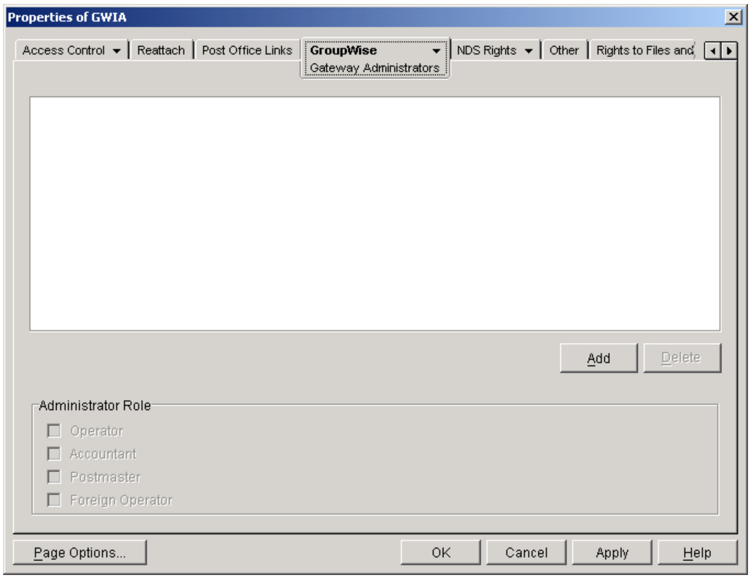
- "Selecting an Accountant" on page 715
- "Enabling Accounting" on page 716
- "Understanding the Accounting File's Fields" on page 717

Selecting an Accountant

You can select one or more GroupWise® users to be accountants. Every day at midnight, each accountant receives an accounting file (acct) that contains information about the messages the gateway sent that day.

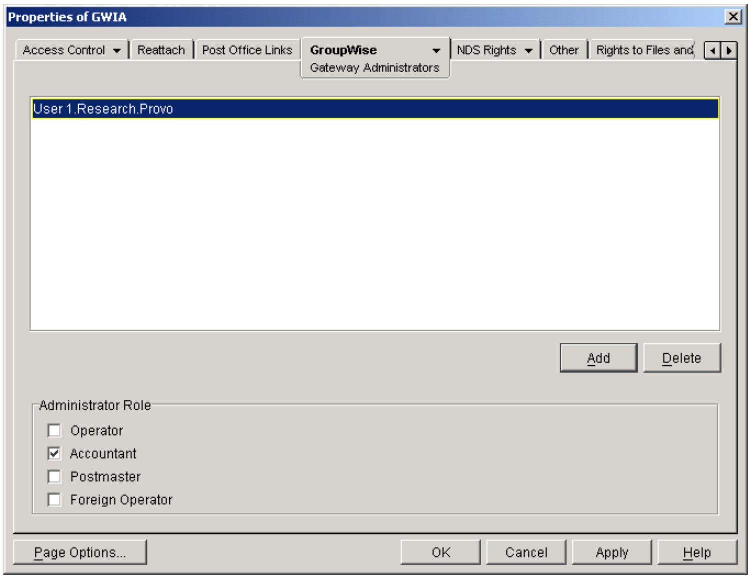
1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click GroupWise > Gateway Administrators to display the Gateway Administrators page.



3 Click Add, browse for and select the user you want to add, then click OK to add the user to the list of administrators.

4 Select the user in the list of administrators, then click Accountant.



Properties of GWIA

User1.Research.Provo

Administrator Role

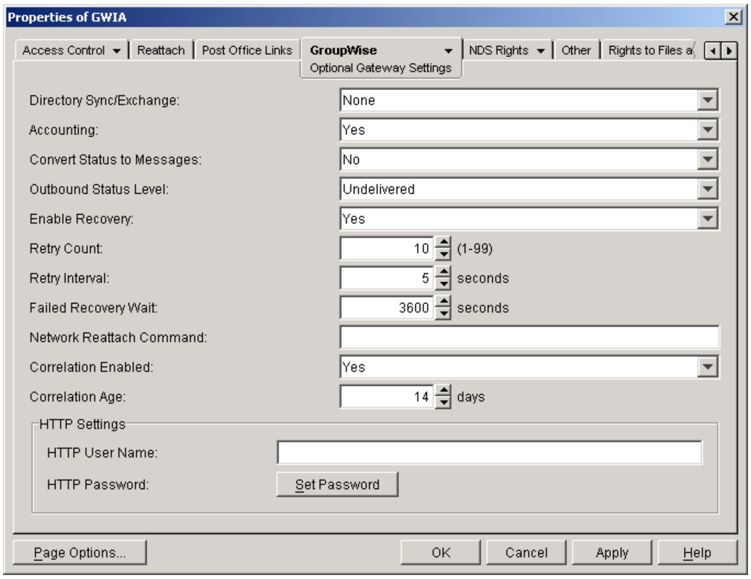
- ☐ Operator
- ☑ Accountant
- ☐ Postmaster
- ☐ Foreign Operator

5 Click OK to save the changes.

Enabling Accounting

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click GroupWise > Optional Gateway Settings to display the Optional Gateway Settings page.



Properties of GWIA

Directory Sync/Exchange:	None
Accounting:	Yes
Convert Status to Messages:	No
Outbound Status Level:	Undelivered
Enable Recovery:	Yes
Retry Count:	10 (1-99)
Retry Interval:	5 seconds
Failed Recovery Wait:	3600 seconds
Network Reattach Command:	
Correlation Enabled:	Yes
Correlation Age:	14 days

HTTP Settings

HTTP User Name:	
HTTP Password:	Set Password

3 Set Accounting to Yes.

4 Set Correlation Enabled to Yes.

5 Click OK.

Understanding the Accounting File’s Fields

The following is an Accounting file entry for a single event. Each field in the entry is described below.

```
O,11/25/2002,21:58:39,3DE29CD2.14E:7:6953,
Mail,2,Provo,Research,jsmith,48909,Meeting
Agenda,Provo,GWIA,sde23a9f.001,MIME,hjones@novell.com,1,2,11388,0
```

Field	Example	Description
Inbound/Outbound	O	Displays I for inbound messages and O for outbound messages
Date	11/25/2004	The date the message was processed.
Time	21:58:39	The time the message was processed.
GroupWise message ID	3DE29CD2.14E:7:6953	The unique GroupWise ID assigned to the message.
GroupWise message type	Mail	Mail message, appointment, task, note, or phone message for outbound messages. Unknown for inbound messages.
GroupWise message priority	2	High priority = 1 Normal priority = 2 Low priority = 3
GroupWise user’s domain	Provo	The domain in which the GroupWise user resides.
GroupWise user’s post office	Research	The post office where the GroupWise user’s mailbox resides.
GroupWise user’s ID	jsmith	The GroupWise user’s ID. For outbound messages, the GroupWise user is the message sender. For inbound messages, the GroupWise user is the message recipient.
GroupWise user’s account ID	48909	The GroupWise user’s account ID. The account ID is assigned on the user’s GroupWise Account page (ConsoleOne > User object > GroupWise tab > Account page).
Message subject	Meeting Agenda	The message’s Subject line. Only the first 32 characters are displayed.
Gateway domain	Provo	The domain where the Internet Agent resides.
Gateway name	GWIA	The Internet Agent’s name.
Foreign message ID	sde23a9f.001	A unique ID for outbound messages. The identifier before the period (sde23a9f) uniquely identifies a message. The identifier after the period (001) is incremented by one for each message sent.
Foreign message type	MIME	The message type (MIME, etc.)

Field	Example	Description
Foreign user’s address	hjones@novell.com	The foreign user’s e-mail address. For inbound messages, the foreign user is the message sender. For outbound messages, the foreign user is the message recipient.
Recipient count	1	The number of recipients.
Attachment count	2	The number of attached files. The total count includes the message.
Message size	11388	The total size, in bytes, of the message and its attachments.
Other	0	Not used.

51 Blocking Unwanted E-Mail

The GroupWise® Internet Agent includes the following features to help you protect your GroupWise system and users from unwanted e-mail:

- "Real-Time Blacklists" on page 719
- "Access Control Lists" on page 721
- "Blocked.txt File" on page 721
- "Mailbomb (Spam) Protection" on page 722
- "SMTP Host Authentication" on page 723
- "Unidentified Host Rejection" on page 723

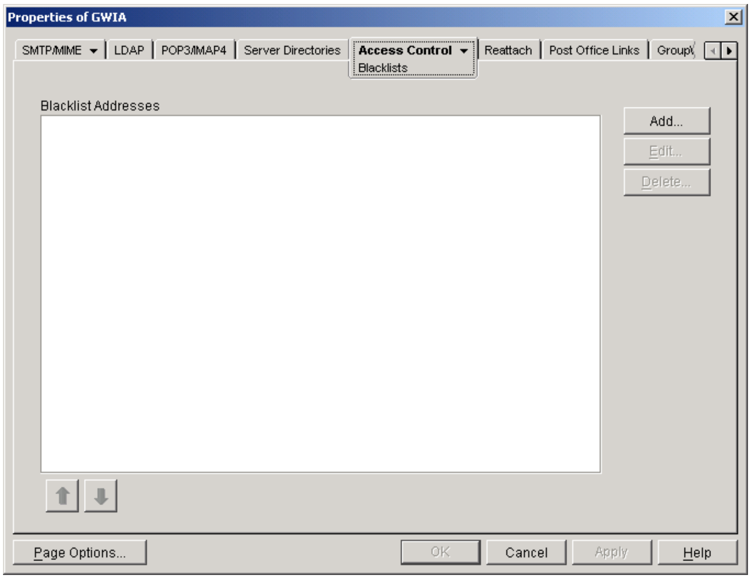
Real-Time Blacklists

Many organizations, such as Mail Abuse Prevention System (MAPS*), Open Relay DataBase (ORDB), and SpamCop*, provide lists of IP addresses that are known to be open relay hosts or spam hosts. If you want to use free blacklist services such as these, or if you subscribe to fee-based services, you can define the blacklist addresses for these services. The Internet Agent will then use the defined services to ensure that no messages are received from blacklisted hosts. The following sections provide information to help you define blacklist addresses and, if necessary, override a host address included in a blacklist.

- "Defining a Blacklist Address" on page 719
- "Overriding a Blacklist" on page 721

Defining a Blacklist Address

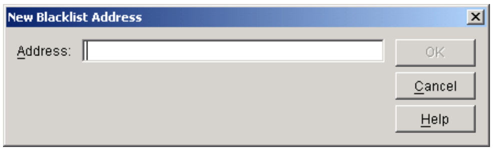
1. In ConsoleOne®, right-click the Internet Agent object, then click Properties.
2. Click Access Control > Blacklists to display the Blacklists page.



The Blacklist Addresses list displays the addresses of all blacklists that the Internet Agent will check when it receives a message from another SMTP host. The Internet Agent checks the first blacklist and continues checking lists until the sending SMTP host's IP address is found or all lists have been checked. If the sending SMTP host's IP address is included on any of the blacklists, the message is rejected. If you have the Internet Agent's logging level set to Verbose, the log file includes information about the rejected message and the referring blacklist.

This list corresponds with the Internet Agent's /rbl switch.

3 Click Add to display the New Blacklist Address dialog box.



The following list provides the names, Web sites, and blacklist addresses for several services that were free at the time of this release:

Service	Site	Address
Mail Abuse Prevention System (MAPS)	www.mail-abuse.org	blackholes.mail-abuse.org
Open Relay DataBase (ORDB)	www.ordb.org	relays.ordb.org
SpamCop	www.spamcop.net	bl.spamcop.net

4 Type the blacklist address in the Address box, then click OK to add the address Blacklist Addresses list.

5 If you have multiple blacklists in the Blacklist Addresses list, use the up-arrow and down-arrow to position the blacklists in the order you want them checked. The Internet Agent checks the blacklists in the order they are listed, from top to bottom.

6 Click OK to save your changes.

Overriding a Blacklist

In some cases, a blacklist might contain a host from which you still want to receive messages. For example, goodhost.com has been accidentally added to a blacklist but you still want to receive messages from that host.

You can use the SMTP Incoming Exceptions list on a class of service to override a blacklist. For information about editing or creating a class of service, see "Creating a Class of Service" on page 706.

Access Control Lists

If you want to block specific hosts yourself rather than use a blacklist (in other words, create your own blacklist), you can configure a class of service that prevents messages from those hosts. You do this on the Internet Agent object's Access Control Settings page by editing the desired class of service to add the hosts to the Prevent Messages From exception list on the SMTP Incoming tab. For example, if you wanted to block all messages from badhost.com, you could edit the default class of service to add badhost.com to the list of prevented hosts.

For information about editing or creating a class of service, see "Creating a Class of Service" on page 706.

Blocked.txt File

ConsoleOne creates a blocked.txt file that includes all the hosts that have been added to the Prevent Messages From exceptions list for the default class of service (see Chapter 49, "Controlling User Access," on page 705).

You can manually edit the blocked.txt file to add or remove hosts. To maintain consistency for your system, you can also copy the list to other Internet Agent installations.

To manually edit the blocked.txt file:

1. Open the blocked.txt file in a text editor.
2. Add the host addresses.

   The entry format is:

   ```
   address1
   address2
   address3
   ```

   where *address* is either a hostname or an IP address. You can block on any octet. For example:

IP Address	Blocks
..*.34	Any IP address ending with 34
172.16.*.34	Any IP address starting with 172.16 and ending with 34
172.16.10-34.*	Any IP address starting with 172.16 and any octet from 10 to 34

   You can block on any segment of the hostname. For example:

Hostname	Blocks
provo*.novell.com	provo.novell.com provo1.novell.com provo2.novell.com
*.novell.com	gw.novell.com (but not novell.com itself)

There is no limit to the number of IP addresses and hostnames that you can block in the blocked.txt file

3 Save the file as blocked.txt.

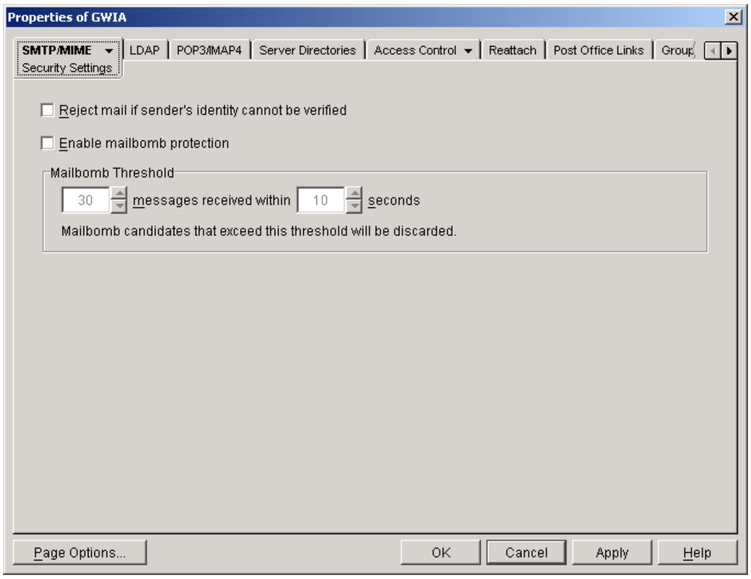
Mailbomb (Spam) Protection

You can protect your system against mailbombs (spam). With mailbomb protection enabled, if the Internet Agent receives a certain number of messages (the default is 30) from the same host or IP address within a specific time interval (the default is 10 seconds), it discards the messages.

To enable mailbomb protection or configure the mailbomb settings:

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click SMTP/MIME > Security Settings to display the Security Settings page.



□ Reject mail if sender's identity cannot be verified

□ Enable mailbomb protection

Mailbomb Threshold

30 messages received within 10 seconds

Mailbomb candidates that exceed this threshold will be discarded.

3 Turn on the Enable Mailbox Protection option.

4 In the Mailbomb Threshold fields, select the message number and time interval to be used.

Any group of messages that exceeds the specified threshold settings will be entirely discarded. If you want to prevent future mailbombs from the mailbomb sender, identify the sender's IP address (by looking at the Internet Agent's console), then modify the appropriate class of service to prevent mail being received from that IP address. For more information, see "Creating a Class of Service" on page 706.

The time setting corresponds to the Internet Agent's /mbtime switch. The message count setting corresponds to the /mbcount switch.

5. Click OK to save your changes.

SMTP Host Authentication

The Internet Agent supports SMTP host authentication for both outbound and inbound message traffic.

- "Outbound Authentication" on page 723
- "Inbound Authentication" on page 723

Outbound Authentication

For outbound authentication to other SMTP hosts, the Internet Agent requires that the remote SMTP hosts support the AUTH LOGIN authentication method. To set up outbound authentication:

1. Include the remote SMTP host's domain name an authentication credentials in the gwauth.cfg file, located in the *domain*\wpgate\gwia directory. The format is:

   ```
   domain_name   authuser   authpassword
   ```

   For example:

   ```
   smtp.novell.com   remotehost   novell
   ```

2. If you have multiple SMTP hosts that require authentication before they will accept messages from your system, create an entry for each host. Make sure to include a hard return after the last entry.

3. If you want to allow the Internet Agent to send messages only to SMTP hosts listed in the gwauth.cfg file, use the following startup switch:

   ```
   /forceoutboundauth
   ```

   With the /forceoutboundauth switch enabled, if a message is sent to an SMTP host not listed in the gwauth.cfg file, the sender will receive an Undeliverable message.

Inbound Authentication

For inbound authentication from other SMTP hosts, you can use the /forceinboundauth startup switch to ensure that the Internet Agent accepts messages only from SMTP hosts that use the AUTH LOGIN authentication method to provide a valid GroupWise user ID and password. The remote SMTP hosts can use any valid GroupWise user ID and password. However, for security reasons, we recommend that you create a dedicated GroupWise user account for remote SMTP host authentication.

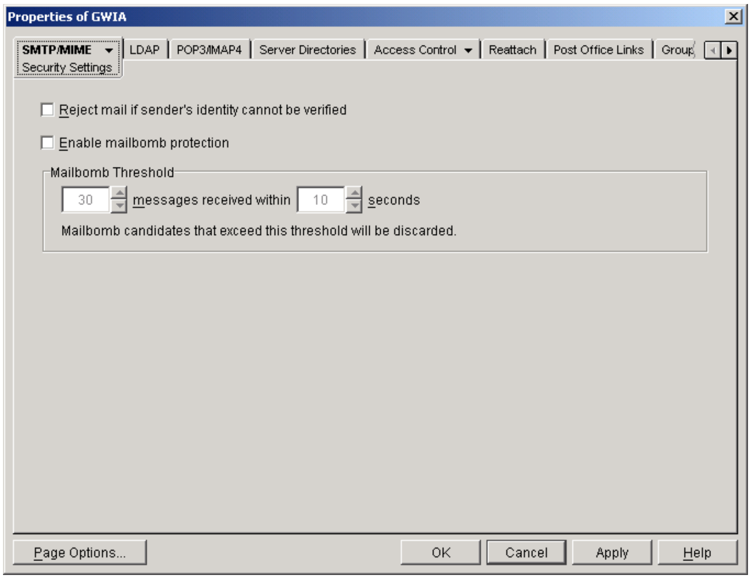
Unidentified Host Rejection

You can have the Internet Agent reject messages from unidentified sources. The Internet Agent will refuse messages from a host if a DNS reverse lookup shows that a "PTR" record does not exist for the IP address of the sender's host.

If you choose not to have the Internet Agent reject messages from unidentified hosts, it will accept messages from any host, but it will display a warning if the sender's host is not authentic.

To configure the Internet Agent to reject messages from unidentified hosts:

1. In ConsoleOne, right-click the Internet Agent object, then click Properties.
2. Click SMTP/MIME > Security Settings to display the Security Settings page.



□ Reject mail if sender's identity cannot be verified

□ Enable mailbomb protection

Mailbomb Threshold

30 messages received within 10 seconds

Mailbomb candidates that exceed this threshold will be discarded.

3. Turn on the Reject Mail if Sender's Identity Cannot Be Verified option.

   This setting corresponds with the Internet Agent's /rejbs switch.
4. Click OK to save your changes.

52 Optimizing Speed and Reliability

The following sections provide information about some of the methods you can use to optimize the speed and reliability of the GroupWise® Internet Agent:

- "Relocating the Internet Agent's Processing Directories" on page 725
- "Increasing Internet Agent Speed" on page 726
- "Automating Reattachment to NetWare Servers" on page 728

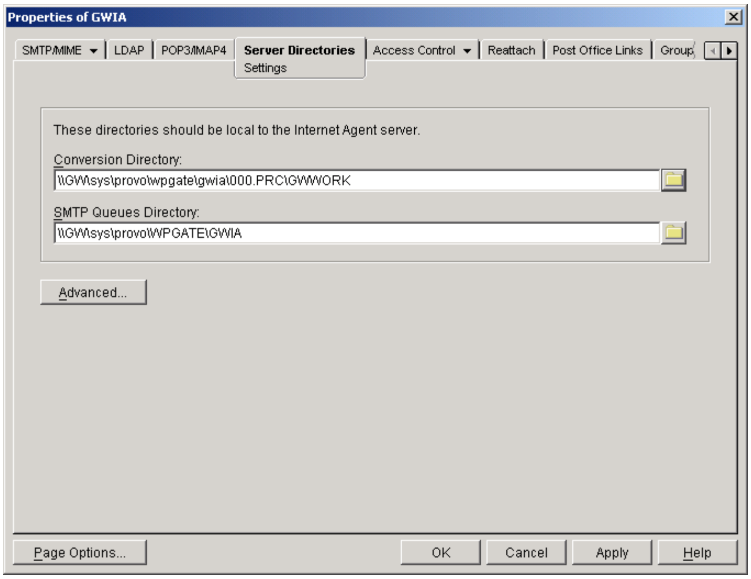
Relocating the Internet Agent's Processing Directories

The Internet Agent uses several directories to process message files. By default, when you install the Internet Agent to a NetWare® server, these directories are created under the Internet Agent's gateway directory (*domain*\wpgate\gwia). To increase performance, you can relocate these directories to the same server as the NetWare Internet Agent.

To define the location of the Internet Agent's directories:

1 In ConsoleOne®, right-click the Internet Agent object, then click Properties.

2 Click Server Directories > Settings to display the Server Directories Settings page.



Properties of GWIA

These directories should be local to the Internet Agent server.

Conversion Directory: \\GW\sys\provo\wpgate\gwia\000.PRC\GWWORK

SMTP Queues Directory: \\GW\sys\provo\WPGATE\GWIA

3 Fill in the fields:

Conversion Directory: Select the directory where the Internet Agent will store temporary files for message conversion. The default directory is the 000.prc\gwwork directory, located under the *domain*\wpgate*gwia* directory when using the NetWare or Linux Internet Agent, or the *c:\grpwise\gwia* directory when using the Windows Internet Agent.

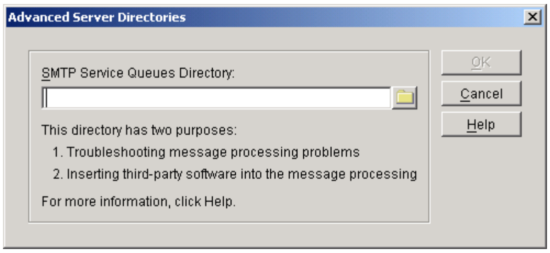
If you type a path to a Windows drive (rather than using the Browse button to select the directory), you must use UNC path syntax.

This setting corresponds with the Internet Agent's /work switch.

SMTP Queues Directory: Select the directory where the Internet Agent will store messages being routed to and from the Internet. The default directory when using the NetWare or Linux Internet Agent is *domain*\wpgate*gwia*. The default directory when using the Windows Internet Agent is the Internet Agent directory on the Windows server (by default, c:\grpwise\gwia). Four subdirectories are created under the SMTP queues directory: defer, send, receive, and result.

This setting corresponds with the Internet Agent's /dhome switch.

4 Click the Advanced button.



This directory has two purposes:
1. Troubleshooting message processing problems
2. Inserting third-party software into the message processing
For more information, click Help.

5 Fill in the field:

SMTP Service Queues Directory: If you want, specify a secondary SMTP queues directory for outbound messages. This secondary directory can be helpful for troubleshooting by providing a way to trap messages before they are routed to the Internet. You can also use the secondary directory to run third-party utilities such as a virus scanner on Internet-bound messages.

The Internet Agent will place all outbound messages in this secondary directory. The messages must then be moved manually (or by another application) to the primary SMTP queues' send directory (see Step 3) before the Internet Agent will route them to the Internet.

This setting corresponds with the /smtphome switch.

If you type a directory path rather than using the Browse button to select a directory, make sure you use UNC path syntax.

6 Click OK to close the dialog box.

7 Click OK to save the changes to the directory locations.

Increasing Internet Agent Speed

You can implement the following procedures to help enhance the Internet Agent's processing speed:

- "Sending and Receiving Threads" on page 727
- "Changing the Maximum Packet Received Buffers" on page 727
- "Increasing Polling Time" on page 727
- "Decreasing the Timeout Cycles" on page 728

Sending and Receiving Threads

The Internet Agent uses sending and receiving threads to process incoming and outgoing messages. The more threads you make available, the more messages the Internet Agent can process concurrently. However, threads place a demand on the station's resources. Too many threads can monopolize memory and CPU utilization.

Make sure you balance your processing speed requirements with the other applications running on the same server as the Internet Agent.

For information about adjusting the SMTP sending and receiving threads, see "Configuring Basic SMTP/MIME Settings" on page 661.

Changing the Maximum Packet Received Buffers

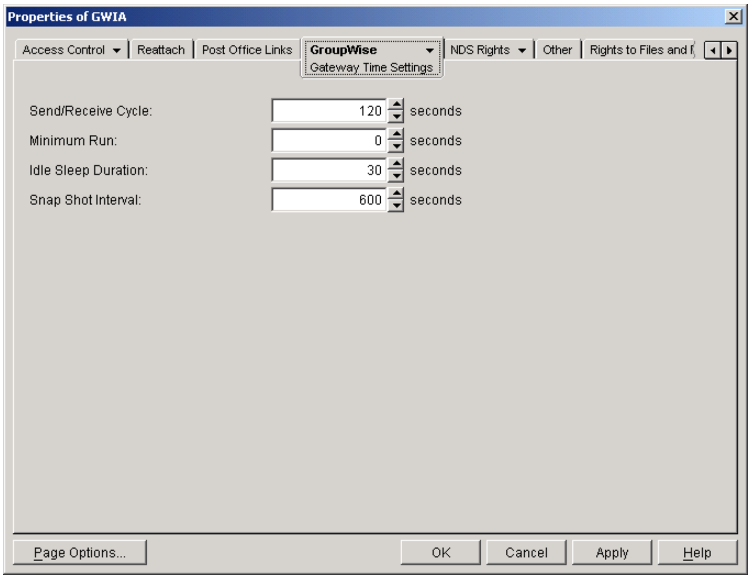
This option is available only for the NetWare version. If you leave the send and receive threads at their default settings, you probably will not need to change the Maximum Packet Received Buffers parameter. However, if you significantly increase the number of send and receive threads, you should increase the default Maximum Packet Received Buffers parameter to better accommodate the SMTP processes. You must change this parameter at the server.

Increasing Polling Time

Incoming and outgoing messages are stored in priority queues. The Internet Agent polls these queues and then forwards the messages for distribution. The Time option lets you control how often the Internet Agent polls these queuing directories. Make sure you balance polling time requirements with the other applications running on the same server as the Internet Agent.

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click GroupWise > Gateway Time Settings to display the Gateway Time Settings page.



Properties of GWIA

Send/Receive Cycle: 120 seconds

Minimum Run: 0 seconds

Idle Sleep Duration: 30 seconds

Snap Shot Interval: 600 seconds

3 Modify the following settings:

Idle Sleep Duration: Select the time, in seconds, you want the Internet Agent to idle after it has processed its queues. A low setting, such as 5 seconds, speeds up processing but requires more resources. A higher setting slows down the Internet Agent but requires fewer resources by reducing the number of network polling scans.

Snap Shot Interval: The Snap Shot Interval is a sliding interval you can use to monitor Internet Agent activity. For example, if the Snap Shot Interval remains at the default (10 minutes), the Snap Shot columns in the console display only the previous 10 minutes of activity.

4 Click OK to save the changes.

Decreasing the Timeout Cycles

The Internet Agent has a series of switches that control its timeout settings. By decreasing the default time of the timeout cycles you may be able to slightly increase the Internet Agent speed. However, the timeout cycles do not place an extremely significant burden on the overall performance of the Internet Agent so the effect may be minimal. You should consider this option only after you have tried everything else.

For information about configuring the timout settings in ConsoleOne, see "Configuring the SMTP Timeout Settings" on page 669. For information about configuring the settings using startup switches, see "Timeouts" on page 786.

Automating Reattachment to NetWare Servers

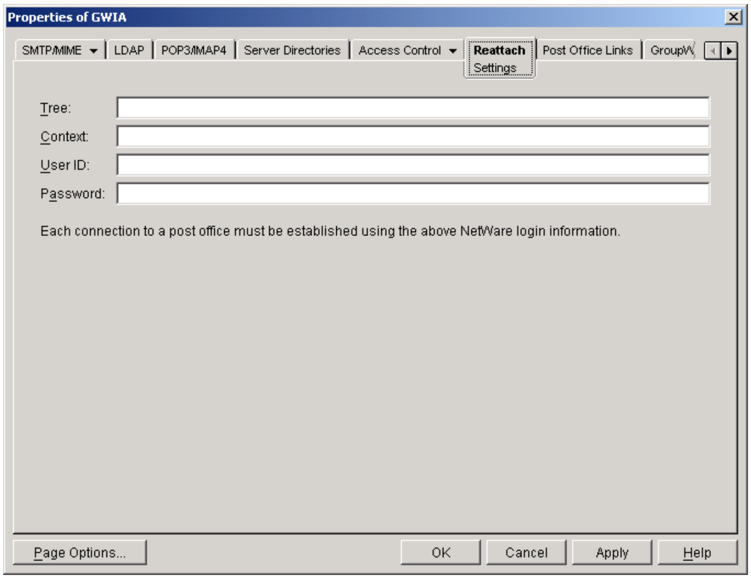
You can specify the reattach information for the Windows Internet Agent in ConsoleOne. Whenever the Windows Internet Agent loses its connection to a post office that is on a NetWare server, it will read the reattach information from the domain database and attempt to reattach to the NetWare server.

The NetWare Internet Agent does not use this information. To reattach to NetWare servers where users' post offices reside, the NetWare Internet Agent uses the user ID and password specified during installation. This user ID and password are entered in the gwia.cfg file. For more information, see "Required Switches" on page 771.

To specify the reattachment information for the Windows Internet Agent:

1 In ConsoleOne, right-click the Internet Agent object, then click Properties.

2 Click Reattach > Settings to display the Reattach Settings page.



Tree:

Context:

User ID:

Password:

Each connection to a post office must be established using the above NetWare login information.

3 Define the following properties:

Tree: Enter the Novell eDirectory™ tree that the Internet Agent logs in to. If the Internet Agent does not use an eDirectory user account, leave this field blank.

Context: Enter the eDirectory context of the Internet Agent's user account. If the Internet Agent does not use an eDirectory user account, leave this field blank.

User ID: Enter the name of the user account.

Password: Enter the password for the user account.

4 Click OK.

53 Monitoring Internet Agent Operations

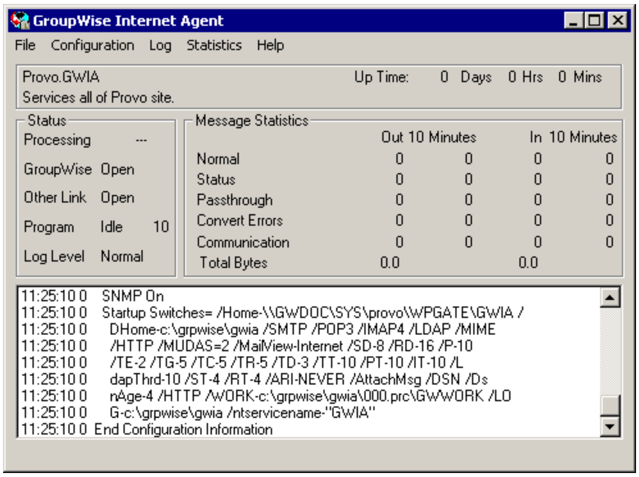
You can monitor the operation of the GroupWise® Internet Agent by using several different diagnostic tools. Each provides important and helpful information about the status of the Internet Agent and how it is currently functioning. Choose from the titles listed below to learn more about how to monitor the operations of the Internet Agent.

- "Monitoring the Internet Agent through the Server Console" on page 731
- "Monitoring the Internet Agent through the Web Console" on page 742
- "Monitoring the Internet Agent through NetWare 6.5 Remote Manager" on page 744
- "Monitoring the Internet Agent through an SNMP Management Console" on page 745
- "Assigning Operators to Receive Warning and Error Messages" on page 745
- "Using Internet Agent Log Files" on page 746
- "Shutting Down the Internet Agent" on page 751

Monitoring the Internet Agent through the Server Console

The Internet Agent console is displayed on the NetWare® server, the Windows server, or Linux where the Internet Agent is running. If the Internet Agent is running as a Windows service under the Local System User, it is displayed on the desktop only if the Allow Service to Interact with Desktop option was selected during installation or has been configured on the Internet Agent service's General property page.

The Internet Agent console on a Windows server is shown below. The console on a NetWare or Linux server displays the same information.



Provo.GWIA Up Time: 0 Days 0 Hrs 0 Mins
Services all of Provo site.

Status

Processing	---	
GroupWise	Open	
Other Link	Open	
Program	Idle	10
Log Level	Normal	

Message Statistics

	Out 10 Minutes		In 10 Minutes	
Normal	0	0	0	0
Status	0	0	0	0
Passthrough	0	0	0	0
Convert Errors	0	0	0	0
Communication	0	0	0	0
Total Bytes	0.0		0.0	

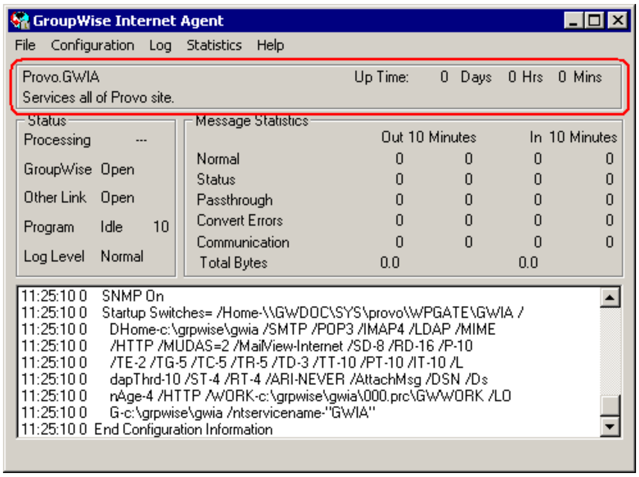
```
11:25:10 0   SNMP On
11:25:10 0   Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIA /
11:25:10 0     DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /MIME
11:25:10 0     /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /P-10
11:25:10 0     /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-10 /L
11:25:10 0     dapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DSN /Ds
11:25:10 0     nAge-4 /HTTP /WORK-c:\grpwise\gwia\000.prc\GWWORK /LO
11:25:10 0     G-c:\grpwise\gwia /ntservicename-"GWIA"
11:25:10 0  End Configuration Information
```

Refer to the following sections for information about the specific sections and functionality included in the console:

- "Description" on page 732
- "Status" on page 732
- "Statistics" on page 733
- "Logging" on page 739
- "Menu Functions" on page 740

Description

The description section of the console, shown below, identifies the Internet Agent and displays how long its has been running.



Provo.GWIA　Up Time: 0 Days 0 Hrs 0 Mins
Services all of Provo site.

Status

Processing	---	
GroupWise	Open	
Other Link	Open	
Program	Idle	10
Log Level	Normal	

Message Statistics

	Out 10 Minutes		In 10 Minutes	
Normal	0	0	0	0
Status	0	0	0	0
Passthrough	0	0	0	0
Convert Errors	0	0	0	0
Communication	0	0	0	0
Total Bytes	0.0		0.0	

```
11:25:10 0   SNMP On
11:25:10 0   Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIA /
11:25:10 0    DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /MIME
11:25:10 0    /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /P-10
11:25:10 0    /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-10 /L
11:25:10 0    dapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DSN /Ds
11:25:10 0    nAge-4 /HTTP /WORK-c:\grpwise\gwia\000.prc\GWWORK /LO
11:25:10 0    G-c:\grpwise\gwia /ntservicename-"GWIA"
11:25:10 0 End Configuration Information
```

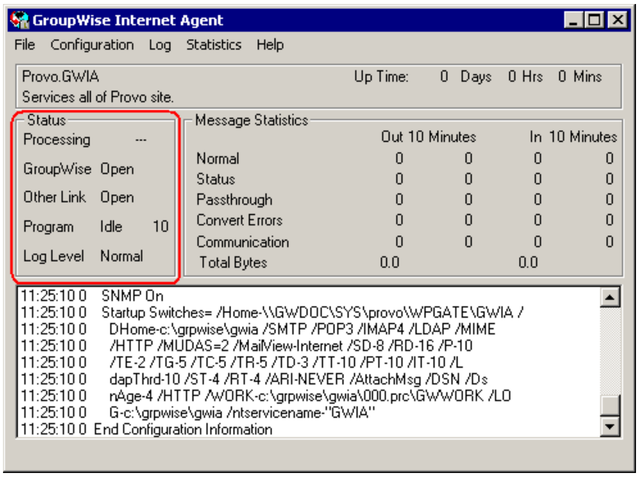
Domain.Gateway: Displays the domain and Internet Agent names.

Up Time: Displays the total length of time the Internet Agent has been running. If the Internet Agent terminates unexpectedly (such as in a power outage), the Up Time display will not reset to 0. It will show the total time elapsed since the Internet Agent was last loaded after a proper termination.

Description: Displays any descriptive information provided on the Internet Agent object's Identification page (Internet Agent object > GroupWise tab > Identification page).

Status

The Status section of the console, shown below, provides a quick look at the Internet Agent's current message processing activity, network connectivity, and information logging level.



```
Provo.GWIA                                  Up Time:    0  Days   0 Hrs   0 Mins
Services all of Provo site.

Status                    Message Statistics
Processing     ---                        Out 10 Minutes       In  10 Minutes
GroupWise  Open           Normal              0        0         0        0
Other Link  Open          Status              0        0         0        0
Program     Idle    10    Passthrough         0        0         0        0
Log Level   Normal        Convert Errors      0        0         0        0
                          Communication       0        0         0        0
                          Total Bytes        0.0                0.0

11:25:10 0   SNMP On
11:25:10 0   Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIA /
11:25:10 0    DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /MIME
11:25:10 0    /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /P-10
11:25:10 0    /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-10 /L
11:25:10 0    dapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DSN /Ds
11:25:10 0    nAge-4 /HTTP /WORK-c:\grpwise\gwia\000.prc\GWWORK /LO
11:25:10 0    G-c:\grpwise\gwia /ntservicename-"GWIA"
11:25:10 0 End Configuration Information
```

Processing: Displays a rotating bar if the Internet Agent is running. If there is no bar, or if the bar is stationary for more than one minute, the Internet Agent is not running.

GroupWise: Displays whether the Internet Agent's network connection is OPEN or CLOSED. This network connection is the Internet Agent's only link to GroupWise. The status indicates whether or not the Internet Agent can write to the wpcsin directory and access the wpcsout directory. The Internet Agent does a scan each cycle to see if these directories exist. If the status is CLOSED, the Internet Agent will attempt to reattach to the network.

It is normal for this field to display the word CLOSED for a minute or so after you start the Internet Agent. However, if the connection remains CLOSED, look for the wpcsin and wpcsout directories. If they are not created yet, start the Message Transfer Agent.

Other Link: This field does not apply to the Internet Agent. It will always say OPEN.

Program: Displays the processing cycle. You can use the Gateway Time Settings page (Internet Agent object > GroupWise tab > Gateway Time Settings page) to adjust the processing cycle.

Log Level: Displays the logging level the Internet Agent is currently using. The logging level determines how much data is displayed on the message portion of this screen and written to the log file. You can use the console menu options to override the default setting for the current session. For information, see "Logging" on page 739

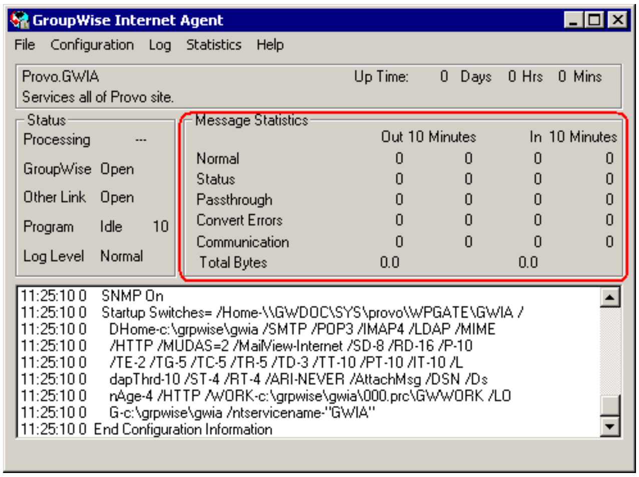
Statistics

The Statistics section of the console can display five different sets of information:

- "Message Statistics" on page 733
- "SMTP Service Statistics" on page 734
- "POP Service Statistics" on page 736
- "IMAP Service Statistics" on page 737
- "LDAP Service Statistics" on page 739

Message Statistics

The Message Statistics section of the console, shown below, is the default statistics section displayed by the Internet Agent console.



Provo.GWIA Up Time: 0 Days 0 Hrs 0 Mins
Services all of Provo site.

Status

Processing	---	
GroupWise	Open	
Other Link	Open	
Program	Idle	10
Log Level	Normal	

Message Statistics

	Out	10 Minutes	In	10 Minutes
Normal	0	0	0	0
Status	0	0	0	0
Passthrough	0	0	0	0
Convert Errors	0	0	0	0
Communication	0	0	0	0
Total Bytes	0.0		0.0	

```
11:25:10 0   SNMP On
11:25:10 0   Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIA /
11:25:10 0    DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /MIME
11:25:10 0    /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /P-10
11:25:10 0    /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-10 /L
11:25:10 0    dapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DSN /Ds
11:25:10 0    nAge-4 /HTTP /WORK-c:\grpwise\gwia\000.prc\GWWORK /LO
11:25:10 0    G-c:\grpwise\gwia /ntservicename-"GWIA"
11:25:10 0 End Configuration Information
```

The Message Statistics shows the number of inbound and outbound messages processed by the Internet Agent. The Out and In columns display the cumulative message totals while the 10 Minutes columns display snap shot totals for the last ten minutes. You change the time interval of the 10 Minutes column in ConsoleOne. For instructions, see "Increasing Polling Time" on page 727.

Normal: Displays the number of inbound and outbound messages processed by the Internet Agent.

Status: Displays the number of inbound and outbound status messages processed by the Internet Agent. The amount of status message traffic depends on the Outbound Status level (ConsoleOne > Internet Agent object > GroupWise tab > Optional Gateway Settings page). If the Outbound Status level is set to Full, more status messages are generated. If the Outbound Status level is set to Undelivered, fewer status messages are generated.

Passthrough: Displays the number of inbound and outbound passthrough messages the Internet Agent has processed.

Convert Errors: Outbound messages are converted from GroupWise® format to MIME or RFC-822 format. Inbound messages are converted to GroupWise format. This field displays the number of inbound and outbound messages that the Internet Agent could not convert.

Communication: Displays the number of communication errors encountered by the Internet Agent.

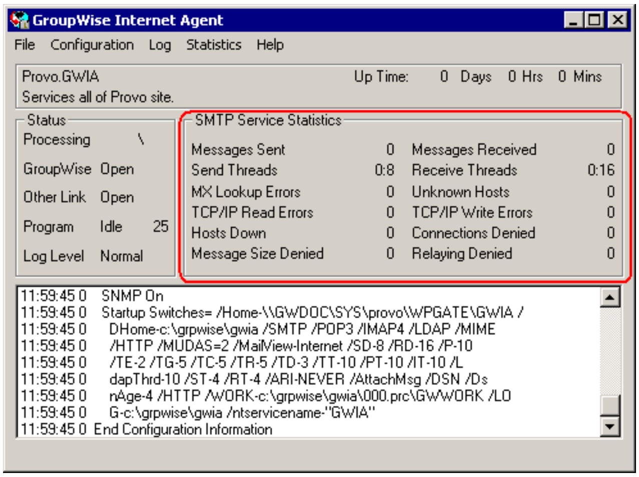
Total Bytes: Displays the total number of bytes of inbound and outbound messages processed by the Internet Agent.

SMTP Service Statistics

The SMTP Service Statistics section, shown below, includes only the information for messages processed by the Internet Agent's SMTP daemon.

In the NetWare Internet Agent's console, press F10-Options, then F9-Stats to switch to the SMTP Service Statistics.

In the Windows Internet Agent's console, select the Statistics menu, then click SMTP Service.



Provo.GWIA Up Time: 0 Days 0 Hrs 0 Mins
Services all of Provo site.

Status

Processing	\	
GroupWise	Open	
Other Link	Open	
Program	Idle	25
Log Level	Normal	

SMTP Service Statistics

Messages Sent	0	Messages Received	0
Send Threads	0:8	Receive Threads	0:16
MX Lookup Errors	0	Unknown Hosts	0
TCP/IP Read Errors	0	TCP/IP Write Errors	0
Hosts Down	0	Connections Denied	0
Message Size Denied	0	Relaying Denied	0

```
11:59:45 0   SNMP On
11:59:45 0   Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIA /
11:59:45 0    DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /MIME
11:59:45 0    /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /P-10
11:59:45 0    /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-10 /L
11:59:45 0    dapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DSN /Ds
11:59:45 0    nAge-4 /HTTP /WORK-c:\grpwise\gwia\000.prc\GWWORK /LO
11:59:45 0    G-c:\grpwise\gwia /ntservicename-"GWIA"
11:59:45 0  End Configuration Information
```

Messages Sent: Displays the total number of SMTP messages sent by the Internet Agent during its current up time.

Send Threads: The first number displays the number of threads currently being used to send SMTP messages. The second number displays the number of threads still available to the Internet Agent for sending SMTP messages. This will be the total number of assigned send threads (by default, 8) minus the currently used threads. You can change the total number of assigned SMTP send threads in ConsoleOne (Internet Agent object > SMTP/MIME tab > Settings page). For more information, see "Configuring Basic SMTP/MIME Settings" on page 661.

Messages Received: Displays the total number of SMTP messages received by the Internet Agent during its current up time.

Receive Threads: The first number is the number of threads currently being used to receive SMTP messages. The second number is the number of threads still available to the Internet Agent for receiving SMTP messages. This will be the total number of assigned receive threads (by default, 16) minus the currently used threads. You can change the total number of assigned SMTP receive threads in ConsoleOne (Internet Agent object > SMTP/MIME tab > Settings page). For more information, see "Configuring Basic SMTP/MIME Settings" on page 661.

MX Lookup Errors: To resolve hostnames to IP addresses, the Internet Agent performs MX record lookups in DNS. This field displays the number of MX record lookups that failed.

Unknown Hosts: Displays the number of SMTP hosts that the Internet Agent could not establish a connection with because the hostname could not be resolved to an IP address.

TCP/IP Read Errors: Displays the number of TCP read errors encountered by the Internet Agent. A TCP read error occurs if the Internet Agent connects successfully to another SMTP host but is unable to process a TCP read command during the message transfer.

TCP/IP Write Errors: Displays the number of TCP write errors encountered by the Internet Agent. A TCP write error occurs if the Internet Agent connects successfully to another SMTP host but is unable to process a TCP write command during the message transfer.

Hosts Down: Displays the number of SMTP hosts that the Internet Agent could not establish a connection with in order to send or receive messages. The Internet Agent was able to resolve the hostname to an IP address, but the connection could not be established.

Connections Denied: Displays the number of connections denied by the Internet Agent. A connection will be denied if the host is blocked through:

- A Class of Service (ConsoleOne > Internet Agent object > Access Control tab > Settings page). For more information, see Chapter 49, "Controlling User Access," on page 705.

- A blacklist (ConsoleOne > Internet Agent object > Access Control tab > Blacklists page). For more information, see Chapter 51, "Blocking Unwanted E-Mail," on page 719.

- The Reject Mail if Sender's Identity Cannot Be Verified setting (ConsoleOne > Internet Agent object > SMTP/MIME tab > Security Settings page), if it is enabled and the sender's identity can not be verified. For more information, see "Protecting Against Unidentified Hosts and Mailbombs (Spam)" on page 668.

Message Size Denied: Displays the number of SMTP messages that the Internet Agent would not send or receive because they exceeded the maximum message size. You can change the maximum message size in ConsoleOne (Internet Agent object > Access Control tab > Settings page > edit class of service > SMTP Incoming tab or SMTP Outgoing tab). For more information, see Chapter 49, "Controlling User Access," on page 705.

Relaying Denied: Displays the number of relay messages denied by the Internet Agent. A relay message will be denied for the following reasons:

- The Internet Agent is not enabled as a relay host (ConsoleOne > Internet Agent object > Access Control tab > SMTP Relay Settings). For more information, see "Enabling SMTP Relaying" on page 674.

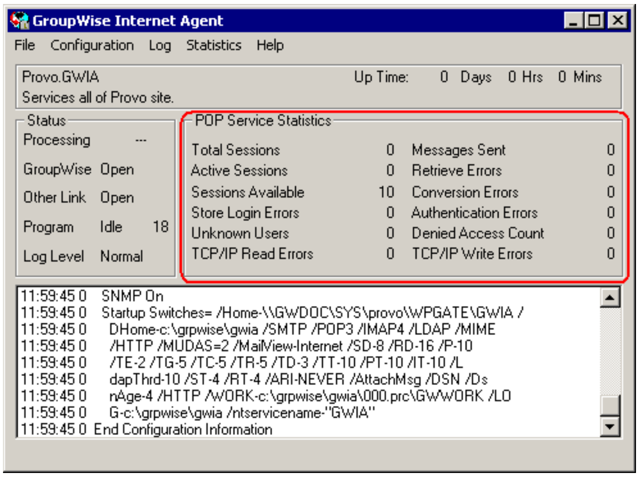
- The relay message could not be authenticated.

POP Service Statistics

The POP Service Statistics section, shown below, provides information about the POP activity handled by the Internet Agent.

In the NetWare Internet Agent's console, press F10-Options, then F9-Stats to switch to the POP Service Statistics.

In the Windows Internet Agent's console, select the Statistics menu, then click POP Service.



Provo.GWIA

Services all of Provo site.

Up Time: 0 Days 0 Hrs 0 Mins

Status

Processing	---	
GroupWise	Open	
Other Link	Open	
Program	Idle	18
Log Level	Normal	

POP Service Statistics

Total Sessions	0	Messages Sent	0
Active Sessions	0	Retrieve Errors	0
Sessions Available	10	Conversion Errors	0
Store Login Errors	0	Authentication Errors	0
Unknown Users	0	Denied Access Count	0
TCP/IP Read Errors	0	TCP/IP Write Errors	0

```
11:59:45 0  SNMP On
11:59:45 0  Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIA /
11:59:45 0   DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /MIME
11:59:45 0   /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /P-10
11:59:45 0   /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-10 /L
11:59:45 0   dapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DSN /Ds
11:59:45 0   nAge-4 /HTTP /WORK-c:\grpwise\gwia\000.prc\GWWORK /LO
11:59:45 0   G-c:\grpwise\gwia /ntservicename-"GWIA"
11:59:45 0 End Configuration Information
```

Total Sessions: Displays the total number of POP3 sessions processed by the Internet Agent during its current up time.

Active Sessions: Displays the number of currently active POP3 sessions.

Sessions Available: Displays the number of threads still available to the Internet Agent for POP3 sessions. This will be the total number of assigned POP3 threads (by default, 10) minus the active sessions. You can change the total number of assigned POP3 threads in ConsoleOne (Internet Agent object > POP3/IMAP4 tab > Settings page). For more information, see Chapter , "Configuring POP3/IMAP4 Services," on page 684.

Messages Sent: Displays the total number of GroupWise mailbox messages retrieved through POP3 sessions.

Retrieve Errors: Displays the number of errors generated because the Internet Agent could not transfer messages to the POP3 client.

Conversion Errors: Displays the number of errors generated because the Internet Agent could not convert retrieved GroupWise messages to MIME format.

Store Login Errors: Displays the number of GroupWise user logins that failed because the users' GroupWise mailboxes were unavailable (for example, the post office is down or the Internet Agent link to the post office is down).

Authentication Errors: Displays the number of GroupWise user logins that failed because the user supplied an incorrect password.

Unknown Users: Displays the number of user logins that failed because the user does not exist in the GroupWise system.

Denied Access Count: Displays the number of POP3 sessions that were denied because the user does not have POP3 access. POP3 access is controlled through the user's Class of Service assignment (ConsoleOne > Internet Agent object > Access Control tab > Settings page). For more information, see Chapter 49, "Controlling User Access," on page 705.

TCP/IP Read Errors: Displays the number of TCP read errors encountered by the Internet Agent. A TCP read error occurs if the Internet Agent successfully opens a POP3 session but is unable to process a TCP read command during the session.

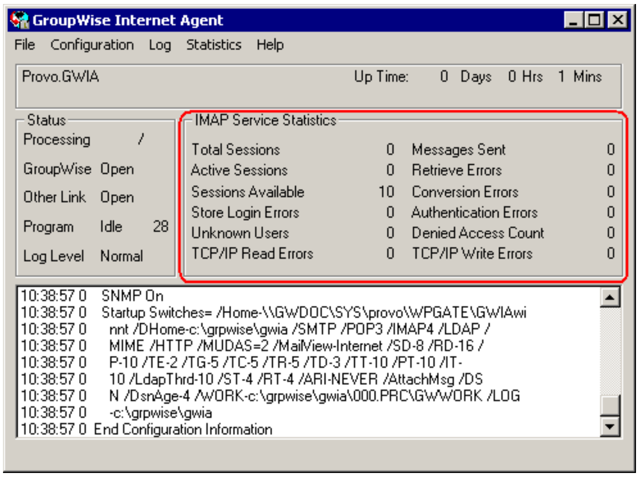
TCP/IP Write Errors: Displays the number of TCP write errors encountered by the Internet Agent. A TCP write error occurs if the Internet Agent successfully opens a POP3 session but is unable to process a TCP write command during the session.

IMAP Service Statistics

The IMAP Service Statistics section, shown below, provides information about the IMAP activity handled by the Internet Agent.

In the NetWare Internet Agent's console, press F10-Options, then F9-Stats to switch to the IMAP Service Statistics.

In the Windows Internet Agent's console, select the Statistics menu, then click IMAP Service.



Provo.GWIA Up Time: 0 Days 0 Hrs 1 Mins

Status

Processing	/	
GroupWise	Open	
Other Link	Open	
Program	Idle	28
Log Level	Normal	

IMAP Service Statistics

Total Sessions	0	Messages Sent	0
Active Sessions	0	Retrieve Errors	0
Sessions Available	10	Conversion Errors	0
Store Login Errors	0	Authentication Errors	0
Unknown Users	0	Denied Access Count	0
TCP/IP Read Errors	0	TCP/IP Write Errors	0

```
10:38:57 0   SNMP On
10:38:57 0   Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIAwi
10:38:57 0    nnt /DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /
10:38:57 0    MIME /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /
10:38:57 0    P-10 /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-
10:38:57 0    10 /LdapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DS
10:38:57 0    N /DsnAge-4 /WORK-c:\grpwise\gwia\000.PRC\GWWORK /LOG
10:38:57 0    -c:\grpwise\gwia
10:38:57 0  End Configuration Information
```

Total Sessions: Displays the total number of IMAP4 sessions processed by the Internet Agent during its current up time.

Active Sessions: Displays the number of currently active IMAP4 sessions.

Sessions Available: Displays the number of threads still available to the Internet Agent for IMAP4 sessions. This will be the total number of assigned IMAP4 threads (by default, 10) minus the active sessions. You can change the total number of assigned IMAP4 threads in ConsoleOne (Internet Agent object > POP3/IMAP4 tab > Settings page). For more information, see Chapter , "Configuring POP3/IMAP4 Services," on page 684.

Messages Sent: Displays the total number of GroupWise mailbox messages retrieved through IMAP4 sessions.

Retrieve Errors: Displays the number of errors generated because the Internet Agent could not transfer messages to the IMAP4 client.

Conversion Errors: Displays the number of errors generated because the Internet Agent could not convert retrieved GroupWise messages to MIME format.

Store Login Errors: Displays the number of GroupWise user logins that failed because the users' GroupWise mailboxes were unavailable (for example, the post office is down or the Internet Agent link to the post office is down).

Authentication Errors: Displays the number of GroupWise user logins that failed because the user supplied an incorrect password.

Unknown Users: Displays the number of user logins that failed because the user does not exist in the GroupWise system.

Denied Access Count: Displays the number of IMAP4 sessions that were denied because the user does not have IMAP4 access. IMAP4 access is controlled through the user's Class of Service assignment (ConsoleOne > Internet Agent object > Access Control tab > Settings page). For more information, see Chapter 49, "Controlling User Access," on page 705.

TCP/IP Read Errors: Displays the number of TCP read errors encountered by the Internet Agent. A TCP read error occurs if the Internet Agent successfully opens a IMAP4 session but is unable to process a TCP read command during the session.

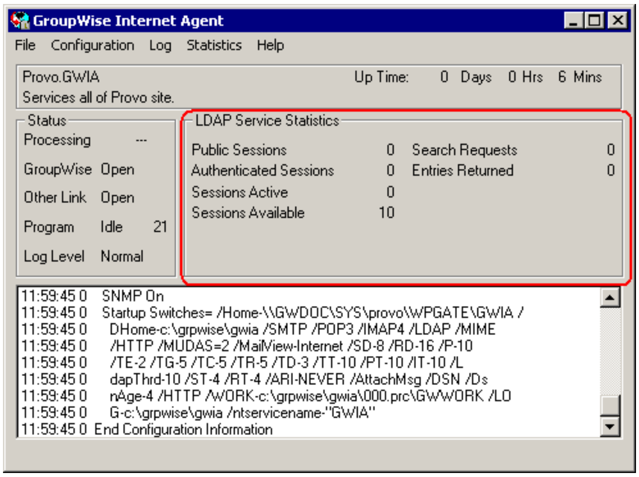
TCP/IP Write Errors: Displays the number of TCP write errors encountered by the Internet Agent. A TCP write error occurs if the Internet Agent successfully opens an IMAP4 session but is unable to process a TCP write command during the session.

LDAP Service Statistics

The LDAP Service Statistics section, shown below, provides information about the LDAP activity handled by the Internet Agent.

In the NetWare Internet Agent's console, press F10-Options, then F9-Stats to switch to the LDAP Service Statistics.

In the Windows Internet Agent's console, select the Statistics menu, then click LDAP Service.



```
Provo.GWIA                                   Up Time:    0  Days   0 Hrs   6  Mins
Services all of Provo site.

Status                         LDAP Service Statistics
Processing      ---            Public Sessions            0   Search Requests     0
GroupWise  Open                Authenticated Sessions     0   Entries Returned    0
Other Link  Open               Sessions Active            0
Program     Idle      21       Sessions Available        10
Log Level   Normal
```

```
11:59:45 0   SNMP On
11:59:45 0   Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIA /
11:59:45 0     DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /MIME
11:59:45 0     /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /P-10
11:59:45 0     /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-10 /L
11:59:45 0     dapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DSN /Ds
11:59:45 0     nAge-4 /HTTP /WORK-c:\grpwise\gwia\000.prc\GWWORK /LO
11:59:45 0     G-c:\grpwise\gwia /ntservicename-"GWIA"
11:59:45 0 End Configuration Information
```

Public Sessions: Displays the total number of LDAP sessions handled by the Internet Agent.

Authenticated Sessions: This field is not used.

Sessions Active: Displays the total number of LDAP sessions currently being processed by the Internet Agent.

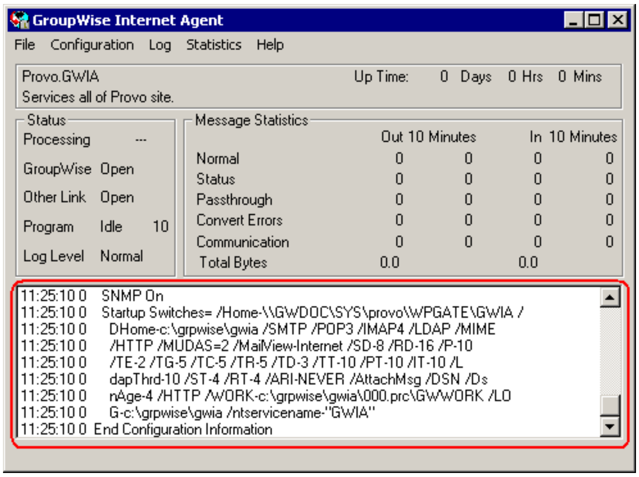
Sessions Available: Displays the number of threads still available to the Internet Agent for LDAP sessions. This will be the total number of assigned LDAP threads (by default, 10) minus the active sessions. You can change the total number of assigned LDAP threads in ConsoleOne (Internet Agent object > LDAP tab > Settings page). For more information, see Chapter , "Configuring LDAP Services," on page 682.

Search Requests: Displays the total number of LDAP queries against the GroupWise Address Book.

Entries Returned: Displays the total number of Address Book entries returned for the search requests. For example, a single search request might return 25 entries.

Logging

The Logging section of the console, shown below, displays Internet Agent activity. The number and detail of these messages depend on the logging level you select. See Chapter , "Using Internet Agent Log Files," on page 746 for more information.



Provo.GWIA Up Time: 0 Days 0 Hrs 0 Mins
Services all of Provo site.

Status

Processing	---	
GroupWise	Open	
Other Link	Open	
Program	Idle	10
Log Level	Normal	

Message Statistics

	Out	10 Minutes	In	10 Minutes
Normal	0	0	0	0
Status	0	0	0	0
Passthrough	0	0	0	0
Convert Errors	0	0	0	0
Communication	0	0	0	0
Total Bytes	0.0		0.0	

```
11:25:10 0   SNMP On
11:25:10 0   Startup Switches= /Home-\\GWDOC\SYS\provo\WPGATE\GWIA /
11:25:10 0    DHome-c:\grpwise\gwia /SMTP /POP3 /IMAP4 /LDAP /MIME
11:25:10 0    /HTTP /MUDAS=2 /MailView-Internet /SD-8 /RD-16 /P-10
11:25:10 0    /TE-2 /TG-5 /TC-5 /TR-5 /TD-3 /TT-10 /PT-10 /IT-10 /L
11:25:10 0    dapThrd-10 /ST-4 /RT-4 /ARI-NEVER /AttachMsg /DSN /Ds
11:25:10 0    nAge-4 /HTTP /WORK-c:\grpwise\gwia\000.prc\GWWORK /LO
11:25:10 0    G-c:\grpwise\gwia /ntservicename-"GWIA"
11:25:10 0  End Configuration Information
```

Menu Functions

The following sections explain the menu options available in the Internet Agent console:

- "NetWare Internet Agent Console" on page 740
- "Windows Internet Agent Console" on page 741

NetWare Internet Agent Console

The menu functions on the NetWare Internet Agent console provide you with the following options.

F6-Restart: Select this option to restart the Internet Agent. The Internet Agent will reread all of its configuration files (gwia.cfg, blocked.txt, gwauth.cfg, route.cfg, and so forth).

F7-Exit: Select this option to terminate the Internet Agent and return to the system prompt.

F8-Info: Select this option to display the Internet Agent configuration information in the Logging section of the console and in the log file.

F9-Browse Log File: Select this option to browse the log file. The following browse options are displayed:

- **F1-Cancel Browse:** Select this option to exit browse mode and to return to the console.
- **F2-Search Log:** Select this option to search for a text string within the log file.
- **Up-arrow, Down-arrow:** Press the Up-arrow and Down-arrow keys to scroll one line at a time.
- **PgUp, PgDn:** Press the Page Up and Page Down keys to scroll one screen at a time.
- **H, H, Up-Arrow:** Press Home, Home, and the Up-arrow to move to the top of the log file.
- **H, H, Down-Arrow:** Press Home, Home, and the Down-arrow to move to the bottom of the log file.

F-10 Options: Select this option to display the options menu. The following options are displayed:

- **F1-Exit Options:** Select this option to return to the main Internet Agent console screen.

- **F2-Log Level:** Select this option to toggle between log levels. This option overrides the default log level set in the Log Settings page (Internet Agent object > GroupWise tab > Log Settings page) or the /loglevel switch in the startup file for the current session.
- **F6-Colors:** Select this option to scroll through the several color options. This option is useful if the Internet Agent station has a monochrome monitor. You can also use this option to help you quickly identify an Internet Agent if more than one is running.
- **F8-Zero Stats:** Select this option to reset the values in the Statistics section of the screen.
- **F9-Stats:** Select this option to scroll through the SMTP service statistics, POP service statistics, IMAP service statistics, and LDAP service statistics.

Windows Internet Agent Console

The menu functions on the Windows Internet Agent console provide you with the following options.

File > Restart (F6): Select this option to restart the Internet Agent. The Internet Agent will reread all of its configuration files (gwia.cfg, blocked.txt, gwauth.cfg, route.cfg and so forth).

File > Exit (F7): Select this option to terminate the Internet Agent and return to the system prompt.

Configuration > Agent Settings (F5): Select this option to display the Internet Agent configuration information.

Configuration > Edit Startup File: Select this option to open the gwia.cfg file in the default text editor.

Log > Cycle Log: Select this option to close the current log file and start a new one.

Log > View Log: Select this option to view the log files.

Log > Log Settings: Select this option to set the logging level, turn on or off disk logging, and configure the maximum log file size and disk space. These changes apply only to the current session.

Statistics > Message: Select this option to display the Message statistics. For information about the Message statistics, see "Message Statistics" on page 733.

Statistics > SMTP Service: Select this option to display the SMTP Service statistics. For information about the SMTP Service statistics, see "SMTP Service Statistics" on page 734.

Statistics > POP Service: Select this option to display the POP Service statistics. For information about the POP Service statistics, see "POP Service Statistics" on page 736.

Statistics > IMAP Service: Select this option to display the IMAP Service statistics. For information about the IMAP Service statistics, see "IMAP Service Statistics" on page 737.

Statistics > LDAP Service: Select this option to display the LDAP Service statistics. For information about the LDAP Service statistics, see "LDAP Service Statistics" on page 739.

Statistics > Zero Statistics (F8): Select this option to reset the Message, SMTP, POP, IMAP, and LDAP statistics.

Monitoring the Internet Agent through the Web Console

You can use a Web browser interface, referred to as the Web console, to monitor the Internet Agent. You cannot use the Internet Agent Web console to change any of the Internet Agent's settings. Changes must be made through ConsoleOne, the server console, or the startup file.

- "Enabling the Web Console" on page 742
- "Monitoring the Internet Agent" on page 743

Enabling the Web Console

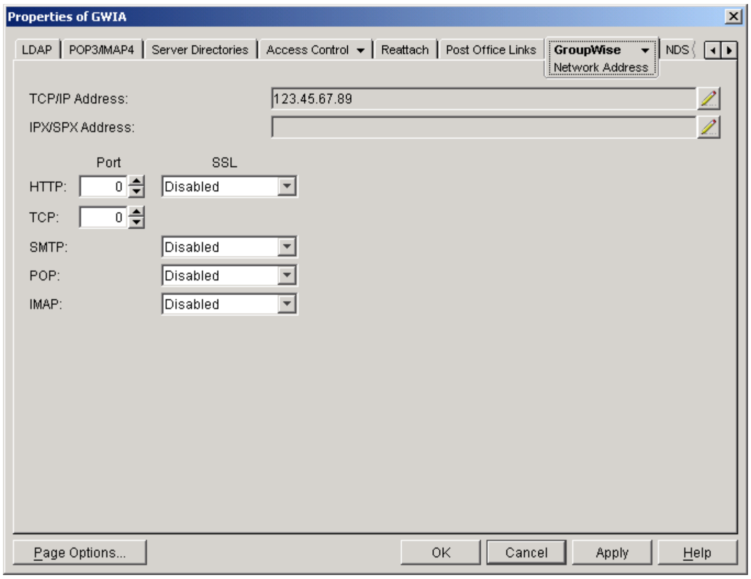
If, during, installation, you enabled the Web console, you can skip this section and continue with the next section, Monitoring the Internet Agent. If you did not, you need to complete the steps in one of the following sections to enable the Web console.

- "Using ConsoleOne" on page 742
- "Using Startup Switches" on page 743

Using ConsoleOne

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

2 Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 123.45.67.89

IPX/SPX Address:

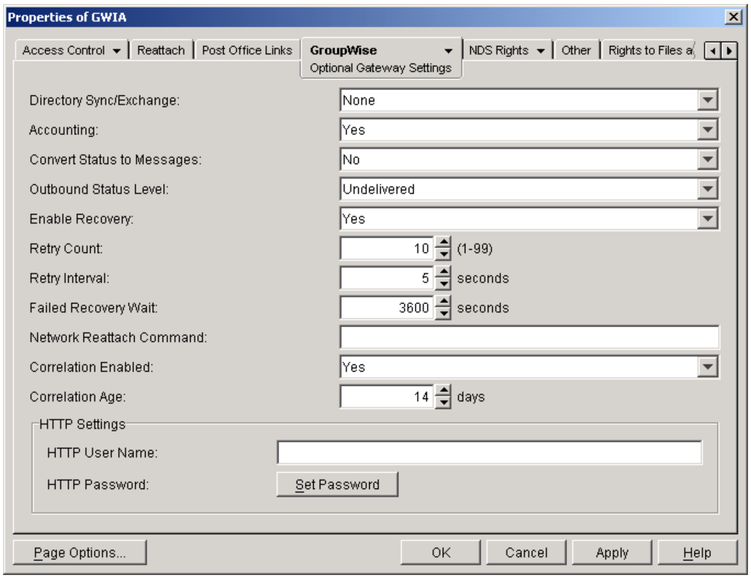
	Port	SSL
HTTP:	0	Disabled
TCP:	0	
SMTP:		Disabled
POP:		Disabled
IMAP:		Disabled

3 In the HTTP Port field, enter a port number. We recommend that you use port 9850 if it is not already in use on the Internet Agent's server.

Assigning a port number enables the Web console; assigning 0 as the port number disables the Web console.

Any user who knows the Internet Agent's IP address (or hostname) and the HTTP port number will be able to use the Web console. If you want to restrict Web console access, you can assign a username and password. To do so:

4 Click the GroupWise tab, then click Optional Gateway Settings to display the Optional Gateway Settings page.



Directory Sync/Exchange: None

Accounting: Yes

Convert Status to Messages: No

Outbound Status Level: Undelivered

Enable Recovery: Yes

Retry Count: 10 (1-99)

Retry Interval: 5 seconds

Failed Recovery Wait: 3600 seconds

Network Reattach Command:

Correlation Enabled: Yes

Correlation Age: 14 days

HTTP Settings

HTTP User Name:

HTTP Password:

5 In the HTTP User Name field, enter an arbitrary username (for example, gwia).

6 Click Set Password to assign a password (for example, monitor).

7 Click OK to save your changes.

Using Startup Switches

You can use the following startup switch in the gwia.cfg file to enable the Web console:

```
/httpport-number
```

We recommend that you use port 9850 if it is not already in use on the Internet Agent's server. For example:

```
/httpport-9850
```

If you want to restrict Web console access to the Internet Agent, you can use the following startup switches to designate a username and password:

```
/httpuser=username /httppassword=password
```

where *username* is an arbitrary name and *password* is any password. For example, you could use "gwia" for the username and "monitor" for the password.

If, during installation, you enabled the Web console, these startup switches were automatically added to the Internet Agent's gwia.cfg file. If the Web console was not enabled during installation, you need to edit the gwia.cfg file and add the switches.

For more information about startup switches, see Appendix 56, "Using Internet Agent Startup Switches," on page 765.

Monitoring the Internet Agent

1 In a Web browser, enter the following:

```
http://IP_address:agent_port (non-secure server)
```

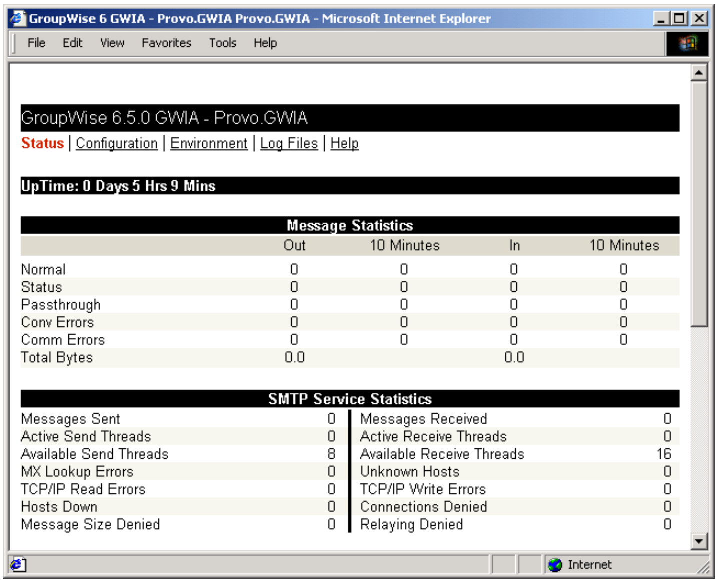
or

```
https://IP_address:agent_port (secure server)
```

where *IP_address* is the IP address or hostname of the server where the Internet Agent is running, and *agent_port* is the port number assigned to the agent. If you used the default port during installation, the port number is 9850.

2 If prompted, enter the Web console username and password.

The Internet Agent Web console is displayed.


GroupWise 6 GWIA - Provo.GWIA Provo.GWIA - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Internet

GroupWise 6.5.0 GWIA - Provo.GWIA

Status | Configuration | Environment | Log Files | Help

UpTime: 0 Days 5 Hrs 9 Mins

Message Statistics

	Out	10 Minutes	In	10 Minutes
Normal	0	0	0	0
Status	0	0	0	0
Passthrough	0	0	0	0
Conv Errors	0	0	0	0
Comm Errors	0	0	0	0
Total Bytes	0.0		0.0	

SMTP Service Statistics

Messages Sent	0	Messages Received	0
Active Send Threads	0	Active Receive Threads	0
Available Send Threads	8	Available Receive Threads	16
MX Lookup Errors	0	Unknown Hosts	0
TCP/IP Read Errors	0	TCP/IP Write Errors	0
Hosts Down	0	Connections Denied	0
Message Size Denied	0	Relaying Denied	0

The Web console has four pages (Status, Configuration, Environment, and Log Files). You can click Help on any page for information about the page.

Monitoring the Internet Agent through NetWare 6.5 Remote Manager

If the Internet Agent is running on a NetWare 6.5 server, you can use the IP Address Management feature in NetWare Remote Manager (NetWare Remote Manager > Manage Server > IP Address Management) to view the IP address and port configuration for the Internet Agent. This is also true for other GroupWise agents (MTA, POA, and WebAccess Agent) running on NetWare 6.5 servers.

IMPORTANT: If the Internet Agent is running in protected mode, it will not display in NetWare Remote Manager.

You access NetWare Remote Manager by entering the following URL in a Web browser:

```
http://server_address:8008
```

For example:

```
http://137.65.123.11:8008
```

For more information about using NetWare Remote Manager, see the NetWare 6.5 documentation (http://www.novell.com/documentation/nw65).

Monitoring the Internet Agent through an SNMP Management Console

The Internet Agent can be monitored through an SNMP management console, such as the one provide with Novell® ZENworks® Server Management.

Before you can monitor the Internet Agent through an SNMP management console, you must compile the Internet Agent's MIB (Management Information Base) file. The Internet Agent's MIB file, named gwia.mib, is located in the agents\snmp directory on the *GroupWise 6.5 Administrator* CD or in the GroupWise® software distribution directory.

The MIB file contains all the Trap, Set, and Get variables used for communication between the Internet Agent and management console. The Trap variables provide warnings that point to current and potential problems. The Set variables allow you to configure portions of the application while it is still running. The Get variables display the current status of different processes of the application.

To compile the MIB file:

1. Copy the Internet Agent MIB (gwia.mib) to the SNMP management console's MIB directory.
2. Compile the MIB file.
3. Create a profile that uses the Internet Agent MIB, then select that profile.

Assigning Operators to Receive Warning and Error Messages

You can select GroupWise users to receive warning and error messages issued by the Internet Agent. Whenever the agent issues a warning or error, these users, called operators, receive a message in their mailboxes. You can specify one or more operators.

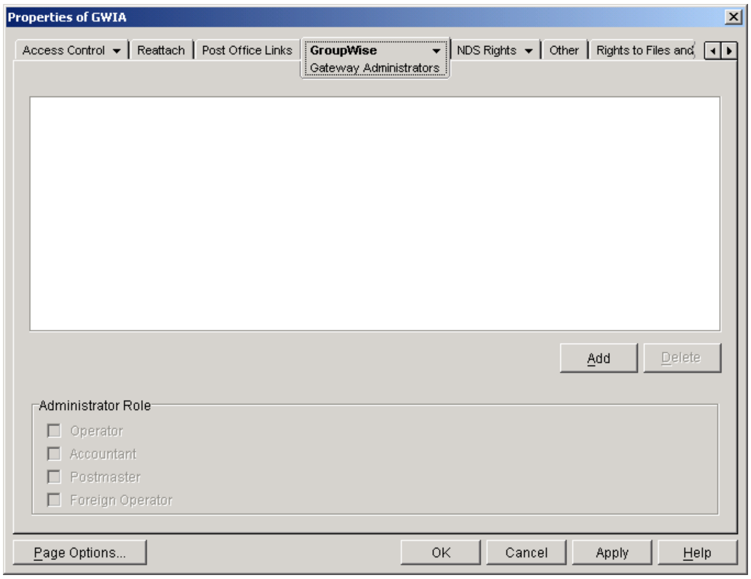
An operator can also shut down the Internet Agent by sending a mail message addressed as follows:

```
gwia:shutdown
```

where *gwia* is your Internet Agent's name.

To assign an operator:

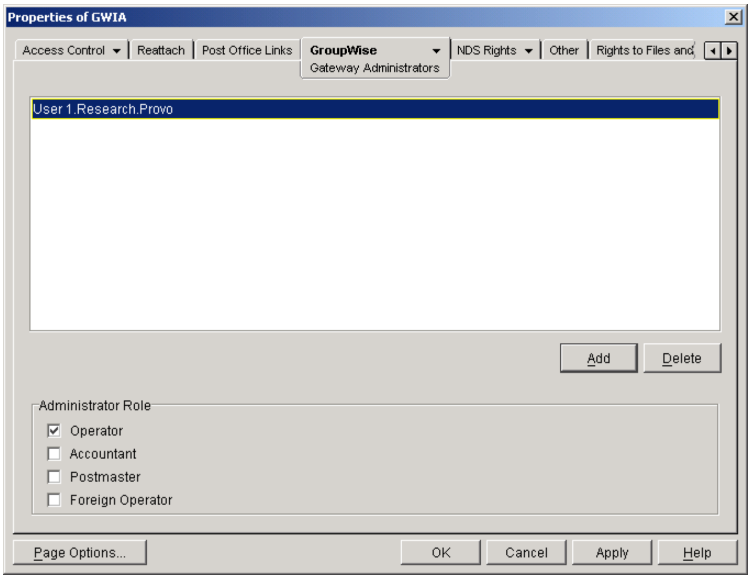
1. In ConsoleOne, right-click the Internet Agent object, then click Properties.
2. Click GroupWise > Gateway Administrators to display the Gateway Administrators page.



Administrator Role

☐ Operator
☐ Accountant
☐ Postmaster
☐ Foreign Operator

3 Click Add, select a user, then click OK to add the user to the Gateway Administrators list.



User 1.Research.Provo

Administrator Role

☑ Operator
☐ Accountant
☐ Postmaster
☐ Foreign Operator

4 Make sure Operator is selected as the Administrator Role.

5 If desired, add additional operators.

6 Click OK.

Using Internet Agent Log Files

You can use the Internet Agent logging options to help you monitor its operation. By default, the Internet Agent logs information to its server console, Web console, and to a log file on disk. You can control the following logging features:

- The type of information to log.
- Disabling disk logging (Windows Internet Agent only).

- How long to retain log files.
- The maximum amount of disk space to use for log files.
- Where to store log files.

You can control logging through ConsoleOne®, Internet Agent startup switches, and the Internet Agent console. The following table shows which logging options you can control from each location.

	ConsoleOne	Startup Switches	NetWare Console	Windows Console
Logging Level	Yes	Yes	Yes	Yes
Disk Logging	No	No	No	Yes
Maximum Log File Age	Yes	Yes	No	Yes
Maximum Disk Space	Yes	Yes	No	Yes
Log File Location	Yes	Yes	No	No

The log settings in ConsoleOne are used as the default settings. Startup switches override the ConsoleOne log settings, and console settings override startup switches. For information about modifying log settings through ConsoleOne, startup switches, or the Internet Agent console, see the following sections:

- "Modifying Log Settings in ConsoleOne" on page 747
- "Modifying Log Settings through Startup Switches" on page 749
- "Modifying Log Settings through the NetWare Internet Agent Console" on page 749
- "Modifying Log Settings through the Windows or Linux Internet Agent Console" on page 749

The following section explains how to view log files created by the Internet Agent:

- "Viewing Log Files" on page 750

Modifying Log Settings in ConsoleOne

Through ConsoleOne, you can configure the following log settings:

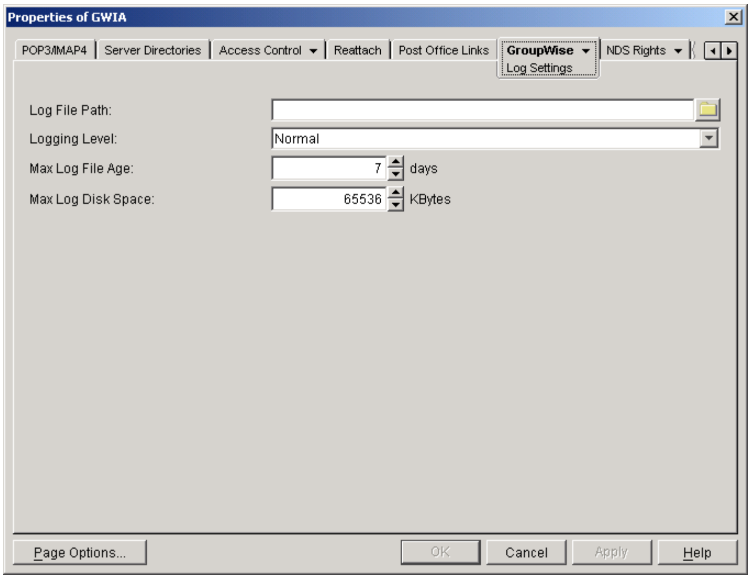
- Log file location
- Logging level (applies to both console logging and disk logging)
- Maximum age for log files
- Maximum disk spaced used for log files

The ConsoleOne settings are the default settings. The Internet Agent will use these settings unless you override them in the gwia.cfg startup file (see "Modifying Log Settings through Startup Switches" on page 749) or the server console (see "Modifying Log Settings through the NetWare Internet Agent Console" on page 749 and "Modifying Log Settings through the Windows or Linux Internet Agent Console" on page 749).

To configure the default log settings in ConsoleOne:

1. Right-click the Internet Agent object, then click Properties.

2 Click GroupWise > Log Settings to display the Log Settings page.



Log File Path:

Logging Level: Normal

Max Log File Age: 7 days

Max Log Disk Space: 65536 KBytes

3 Modify any of the following properties:

Log File Path: The Internet Agent creates a new log file each day and each time it is started. The log file is named *mmdd*gwia.*nnn*, where *mm* is the month, *dd* is the day, and *nnn* is a sequenced number (001 for the first log file of the day, 002 for the second, and so forth).

By default, the log files will be saved to the *domain*\wpgate*gwia*\000.prc directory for the NetWare® Internet Agent, c:\*grpwise**gwia* for the Windows Internet Agent, or /var/log/novell/groupwise/*domain_name*.gwia for Linux. If you want to specify a different location, enter the directory path or browse to and select the directory.

Logging Level: There are four logging levels:

- **Off:** Disables the logging function.
- **Normal:** Displays warnings and error messages. This is the preferred logging level.
- **Verbose:** Displays information about traffic, including non-delivery reports, in addition to warnings and error messages. Information includes the filename, path, message ID, and size of the message being processed; the IP address of any inbound SMTP connections; the Internet Agent-specific MSG number; and SMTP connection messages such as “Connect to novell.com” and “Accepted connection from 172.16.5.18 novell.com”.
- **Diagnostic:** Displays detailed function calls made by the Internet Agent. This level is not useful for most troubleshooting. Verbose is better for standard troubleshooting.

The verbose and diagnostic logging levels do not degrade Internet Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Max Log File Age: Specify the number of days you want the Internet Agent to retain old log files. The Internet Agent will retain the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.

Max Log Disk Space: Specify the maximum amount of disk space you want to use for log files. If the disk space limit is exceeded, the Internet Agent will delete log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 65536 KB.

4 Click OK to save the log settings.

Modifying Log Settings through Startup Switches

You can use startup switches to override any log settings you configured in ConsoleOne. See "Modifying Log Settings in ConsoleOne" on page 747.

To use a switch, you can:

- Add the switch to the command line. For example:

```
load gwia.nlm /ph-j:\domain\wpgate\gwia /loglevel-verbose
```

- Include the switch in the gwia.cfg file. The gwia.cfg file is located in the same directory as the Internet Agent program (typically sys:\system, c:\grpwise\gwia, or \domain\wpgate\gwia).

For information about the startup switches that can be used to modify log settings, see "Log File Switches" on page 800.

Modifying Log Settings through the NetWare Internet Agent Console

You can use the NetWare Internet Agent console to set the logging level for the current session.

Changes you make to logging level at the console apply only to the current session. When you restart the Internet Agent, the logging level is reset to the settings specified in ConsoleOne or the startup switches. See "Modifying Log Settings in ConsoleOne" on page 747 and "Modifying Log Settings through Startup Switches" on page 749.

To modify the logging level:

1. At the NetWare Internet Agent's console, press F10-Options, then press F2-Log Level repeatedly to toggle among the available log levels:
   - **Off:** Disables the logging function.
   - **Normal:** Displays warnings and error messages. This is the preferred logging level.
   - **Verbose:** Displays information about traffic, including non-delivery reports, in addition to warnings and error messages. Information includes the filename, path, message ID, and size of the message being processed; the IP address of any inbound SMTP connections; the Internet Agent-specific MSG number; and SMTP connection messages such as "Connect to novell.com" and "Accepted connection from 172.16.5.18 novell.com".
   - **Diag:** Displays detailed function calls made by the Internet Agent. This level is not useful for most troubleshooting. Verbose is better for standard troubleshooting.
2. Press F1-Exit Options to return to the main console screen.

Modifying Log Settings through the Windows or Linux Internet Agent Console

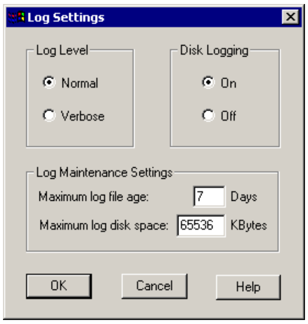
You can use the Windows Internet Agent console to override the following log settings for the current sessions:

- Disk logging on/off
- Log file location
- Logging level (applies to both console logging and disk logging)
- Maximum age for log files
- Maximum disk spaced used for log files

Changes you make to the log settings at the console apply only to the current session. When you restart the Internet Agent, the log level is reset to the level specified in ConsoleOne or the startup switches. See "Modifying Log Settings in ConsoleOne" on page 747 and "Modifying Log Settings through Startup Switches" on page 749.

To modify the log settings:

1. In the Windows Internet Agent console, click the Log menu > Log Settings to display the Log Settings dialog box.



Log Settings

Log Level

● Normal

○ Verbose

Disk Logging

● On

○ Off

Log Maintenance Settings

Maximum log file age: 7 Days

Maximum log disk space: 65536 KBytes

2. Change the desired settings:

   - **Log Level:** Select Normal to display warnings and error messages; this is the preferred logging level. Select Verbose to display information about traffic, including non-delivery reports, in addition to warnings and error messages. Information includes the filename, path, message ID, and size of the message being processed; the IP address of any inbound SMTP connections; the Internet Agent-specific MSG number; and SMTP connection messages such as "Connect to novell.com" and "Accepted connection from 172.16.5.18 novell.com".
   - **Disk Logging:** Select On or Off to enable or disable logging of information to log files.
   - **Maximum Log File Age:** Specify the number of days you want the Internet Agent to retain old log files. The Internet Agent will retain the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.
   - **Maximum Log Disk Space:** Specify the maximum amount of disk space you want to use for log files. If the disk space limit is exceeded, the Internet Agent will delete log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 65536 KB.

Viewing Log Files

You can view the log file for the current session, or you can view archived log files. The current log file is viewable only through the Internet Agent console or Internet Agent Web console; archived files are viewable through the consoles or an ASCII text editor.

Current Log File

The current log file is displayed in the Logging window of the Internet Agent console, with only the most current operations visible. The log file is complete, and includes the gateway startup and configuration information and ongoing operations logged by time, including the shutdown operation. You can browse the file from top to bottom or perform a search for any text string you want. You can also view the current log file from the Internet Agent Web console.

Archived Log Files

The Internet Agent creates a new log file every day at midnight or every time it restarts. Older log files are not deleted for at least one day unless you have not allowed sufficient disk space for them to be archived.

Log files are named according to the date they were created. If the Internet Agent was restarted during the day, the file extension will indicate which session is logged (for example 0317log.003 indicates the third session logged for March 17).

Archived log files are saved in ASCII. You can use any text editor to open a file or to print it. You can also view the log files from the Internet Agent console or the Internet Agent Web console.

Shutting Down the Internet Agent

The following sections describe the various methods you can use to shut down the Internet Agent:

- "Using the Console" on page 751
- "Using a Mail Message" on page 751
- "Using a Shutdown File" on page 751

Using the Console

To shut down the Internet Agent while at the server console:

1 In the NetWare Agent console, press F7-Exit, then select Yes.

or

In the Windows Agent, click the File menu > Exit.

Using a Mail Message

The Internet Agent can be shut down by sending a shutdown message to the Internet Agent. In order to shut down the program with a message, the user sending the message must be defined as an operator for the Internet Agent. This prevents unauthorized users from shutting down the Internet Agent. For information about defining a user as an operator, see "Assigning Operators to Receive Warning and Error Messages" on page 745.

The message to shut down the Internet Agent must be addressed to the Internet Agent, not a non-GroupWise domain. The syntax for the To line is:

```
gwia:shutdown
```

where *gwia* is the name of the Internet Agent object.

Using a Shutdown File

The Internet Agent can also be unloaded by placing a file named shutdown in the *domain*\wpgate\gwia\000.prc directory. When the Internet Agent sees this file, it will delete the file and shut down.

54 Securing Internet Agent Connections Via SSL

The Internet Agent can use the SSL (Secure Socket Layer) protocol to enable secure connections to other SMTP hosts, POP/IMAP clients, and the Internet Agent Web console. For the Internet Agent to do so, you must ensure that it has access to a server certificate file and that you've configured which connection types (SMTP, POP, IMAP, HTTP) you want secured through SSL. The following sections provide instructions:

- "Defining the Certificate File" on page 753
- "Defining Which Connections Will Use SSL" on page 754

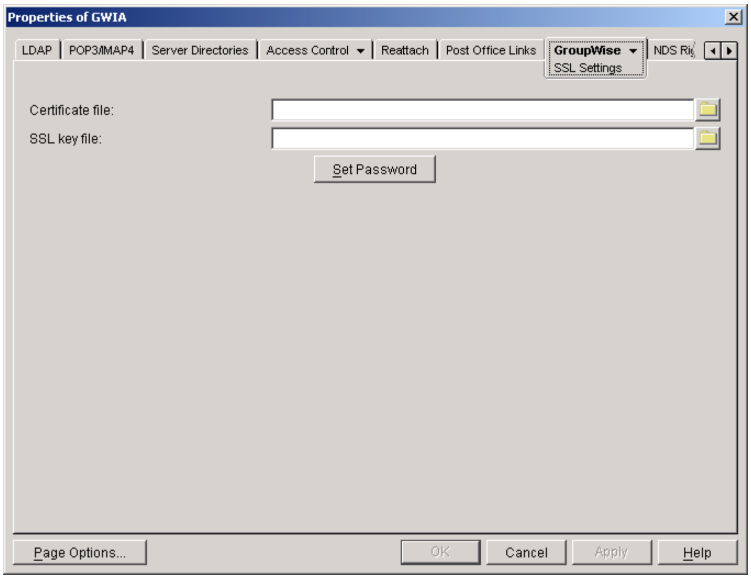
Defining the Certificate File

To use SSL, the Internet Agent requires access to a server certificate file and key file. The Internet Agent can use any Base64/PEM or PFX formatted certificate file located on its server. If the Internet Agent's server does not have a server certificate file, you can use the GroupWise Generate CSR utility to help you obtain one. For information, see "GroupWise Generate CSR Utility (GWCSRGEN)" on page 79.

To define the certificate file and key file that the Internet Agent will use:

1 In ConsoleOne®, right-click the Internet Agent object, then click Properties.

2 Click GroupWise > SSL Settings to display the SSL Settings page.



3 Fill in the Certificate File, SSL Key File, and Set Password fields:

Certificate File: Specify the server certificate file that the Internet Agent will use. The certificate file must be in Base64/PEM or PFX format. If you type the filename rather than using the Browse button to select it, use the full path if the file is not in the same directory as the Internet Agent program. This setting corresponds to the Internet Agent's /certfile switch.

SSL Key File: Specify the key file associated with the certificate. If the private key is included in the certificate file rather than in a separate key file, leave this field blank. If you type the filename rather than using the Browse button to select it, use the full path if the file is not in the same directory as the Internet Agent program. This setting corresponds to the Internet Agent's /keyfile switch.

Set Password: Click Set Password to specify the password for the key. If the key does not require a password, do not use this option. This setting corresponds to the /keypasswd switch.

4 If you want to define which connections (HTTP, SMTP, POP3, or IMAP4) will use SSL, click Apply to save your changes, then continue with the next section, "Defining Which Connections Will Use SSL" on page 754.

or

Click OK to save your changes.

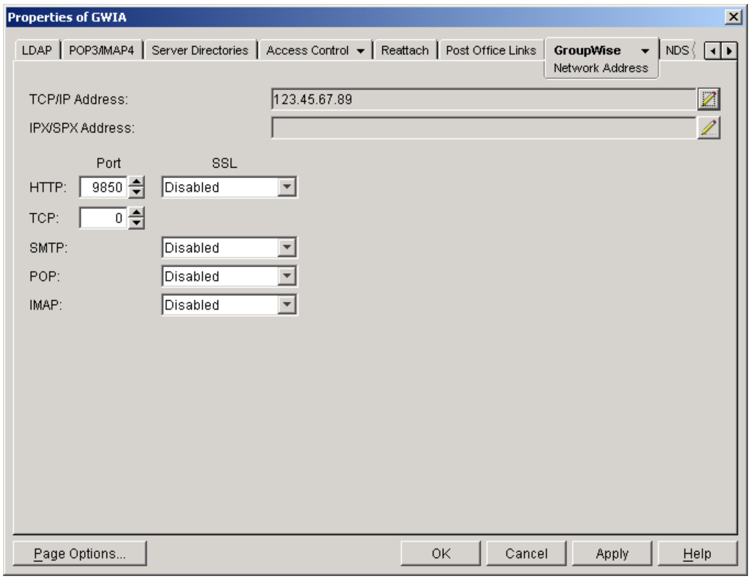
Defining Which Connections Will Use SSL

After you've defined the Internet Agent's certificate and key file (see "Defining the Certificate File" on page 753), you can configure which connections you want to use SSL. You can enable SSL connections to other SMTP hosts and the Internet Agent Web console, which means that an SSL connection will be used if the other SMTP host or the Web browser (running the Web console) supports SSL. You can also enable or require SSL connections to POP3 and IMAP4 clients. If SSL is enabled, an SSL connection is used if the client supports SSL; if SSL is required, only SSL connections will be accepted.

To configure connections to use SSL:

1 In ConsoleOne, if the Internet Agent object's property pages are not already displayed, right-click the Internet Agent object, then click Properties.

2 Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 123.45.67.89

IPX/SPX Address:

	Port	SSL
HTTP:	9850	Disabled
TCP:	0	
SMTP:		Disabled
POP:		Disabled
IMAP:		Disabled

3 Configure the SSL settings for the following connections:

HTTP: Select Enabled to enable the Internet Agent to use a secure connection when passing information to the Internet Agent Web console. The Web browser must also be enabled to use SSL; if it is not, a non-secure connection will be used.

SMTP: Select Enabled to enable the Internet Agent to use a secure connection to other SMTP hosts. The SMTP host must also be enabled to use SSL or TLS (Transport Layer Security); if it is not, a non-secure connection will be used.

POP: Select from the following options to configure the Internet Agent's use of secure connections to POP clients:

- **Disabled:** The Internet Agent will not support SSL connections. All connections will be non-SSL through port 110.
- **Enabled:** The POP client determines whether an SSL connection or non-SSL connection is used. The Internet Agent will listen for SSL connections on port 995 and non-SSL connections on port 110.
- **Required:** The Internet Agent will force SSL connections on port 995 and port 110. Non-SSL connections will be denied.

IMAP: Select from the following options to configure the Internet Agent's use of secure connections to IMAP clients:

- **Disabled:** The Internet Agent will not support SSL connections. All connections will be non-SSL through port 143.
- **Enabled:** The IMAP client determines whether an SSL connection or non-SSL connection is used. The Internet Agent will listen for SSL connections on port 993 and non-SSL connections on port 143.
- **Required:** The Internet Agent will force SSL connections on port 993 and port 143. Non-SSL connections will be denied.

55 Connecting GroupWise Systems and Domains Using the Internet Agent

The Internet Agent can be used as a link between GroupWise systems and between domains in the same GroupWise system.

- "Connecting GroupWise Systems" on page 757
- "Linking Domains" on page 762

Connecting GroupWise Systems

If you have two independent GroupWise systems, you can use the Internet Agent to connect the two systems. This requires each GroupWise system to have the Internet Agent installed.

After the systems are connected, you can synchronize information between the two systems so that users from both systems appear in the GroupWise Address Book.

The following sections provide instructions:

- "Overview" on page 757
- "Creating an External Domain" on page 758
- "Linking to the External Domain" on page 759
- "Checking the Link Status of the External Domain" on page 761
- "Sending Messages Between Systems" on page 762
- "Exchanging Information Between Systems" on page 762

Overview

For the purpose of the following discussion, GWSys1 and GWSys2 represent two separate GroupWise systems.

When you connect the two systems, you connect the two domains where the Internet Agents are located. To do so, you will:

- In GWSys1, define the GWSys2 Internet Agent domain as an external domain. Configure a domain link from the GWSys1 Internet Agent domain to the external domain, defining the link type as a gateway link that uses the Internet Agent. This allows GWSys1 to deliver messages to GWSys2.
- In GWSys2, define the GWSys1 Internet Agent domain as an external domain. Configure a domain link from the GWSys2 Internet Agent domain to the external domain, defining the link type as a gateway link that uses the Internet Agent. This allows GWSys2 to deliver messages to GWSys1.

After you've connected the two systems, users can send messages between the two systems by entering the recipients' full addresses (*userID.post_office.domain* or *user@host*).

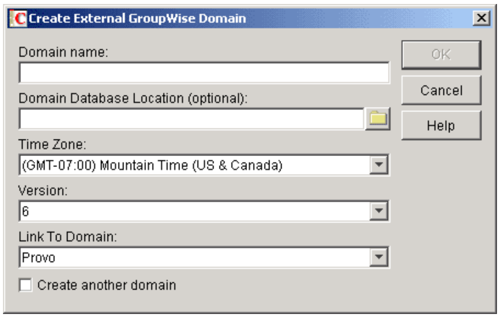
If desired, you can simplify addressing by exchanging information between systems, which causes user information to be displayed in the Address Book. The easiest way to exchange information is to enable the External System Synchronization feature in both systems. When enabled, this synchronization constantly updates the Address Books in both systems so that local users can more easily address messages to and access information about the users in the external system. If you don't want to enable the External System Synchronization feature, you can manually exchange information.

Creating an External Domain

The first step in connecting two GroupWise systems via Internet Agents is to create an external domain in each GroupWise system. The external domain represents the Internet Agent domain in the other GroupWise system and provides the medium through which you define the link to the other system.

To create an external domain:

1. In ConsoleOne®, right-click GroupWise System (in the left-pane), click New > External Domain to display the Create External GroupWise Domain dialog box.



Domain name:

Domain Database Location (optional):

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Version: 6

Link To Domain: Provo

□ Create another domain

2. Fill in the following fields:

   Domain Name: Enter the name of the Internet Agent domain as it is defined in the external GroupWise system.

   Domain Database Location (Optional): Leave this field empty.

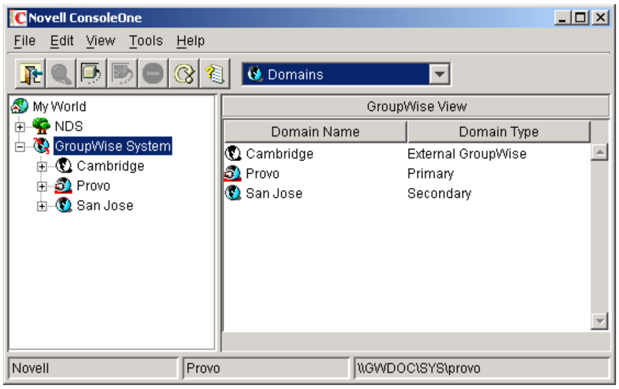
   Time Zone: Select the time zone where the domain is physically located.

   Version: Select the external domain's GroupWise version. The domain's version is determined by its MTA version. The options are 4.X, 5.X, and 6.

   Link to Domain: Select the domain in your system that you want to link to the external domain. This must be your system's Internet Agent domain. By default, all messages sent to the external GroupWise system will be routed to this domain. The domain's MTA will then route the messages to the Internet Agent, which will connect to the Internet Agent in the other system.

3. Click OK to create the external domain.

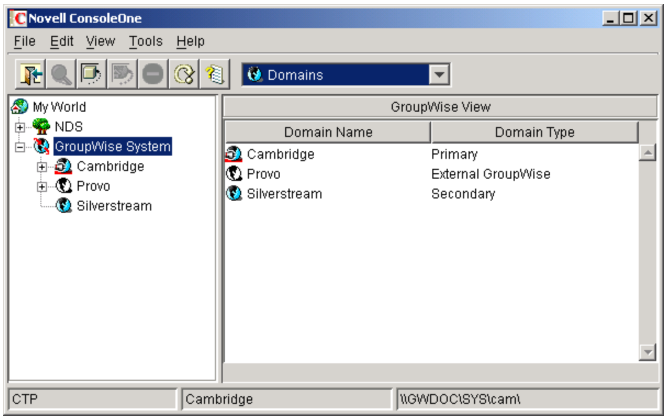
   The external domain is added to your GroupWise system and is visible in the GroupWise View. In the following example, Cambridge is the external domain.



Domain Name	Domain Type
Cambridge	External GroupWise
Provo	Primary
San Jose	Secondary

Novell | Provo | \\GWDOC\SYS\provo

4 Repeat Step 1 through Step 3 to define an external domain in the second GroupWise system. If you do not have administrative rights to that system, you will need to coordinate with that GroupWise system's administrator.



Domain Name	Domain Type
Cambridge	Primary
Provo	External GroupWise
Silverstream	Secondary

CTP | Cambridge | \\GWDOC\SYS\cam\

5 Continue with the next section, Linking to the External Domain.

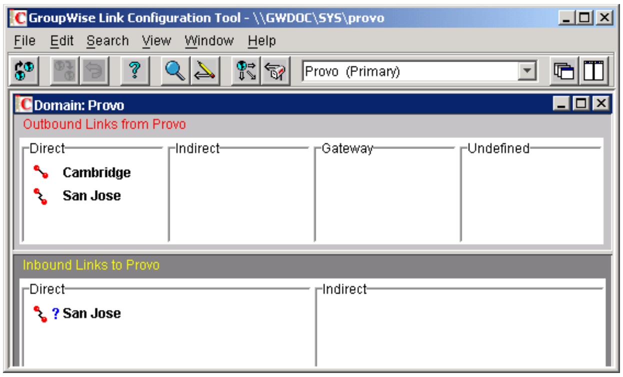
Linking to the External Domain

After you define a domain from the other GroupWise system as an external domain in your system, you need to make sure that your system's domains have the appropriate links to the external domain.

The Internet Agent domain in your system needs to have a gateway link to the external domain. All other domains in your system will have indirect links (through the Internet Agent domain) to the external domain. These links are configured automatically when the external domain was created.

To configure the gateway link for your Internet Agent domain:

1 In ConsoleOne, right-click the Internet Agent domain, click GroupWise Utilities > Link Configuration to display the Link Configuration utility.



GroupWise Link Configuration Tool - \\GWDOC\SYS\provo

Domain: Provo

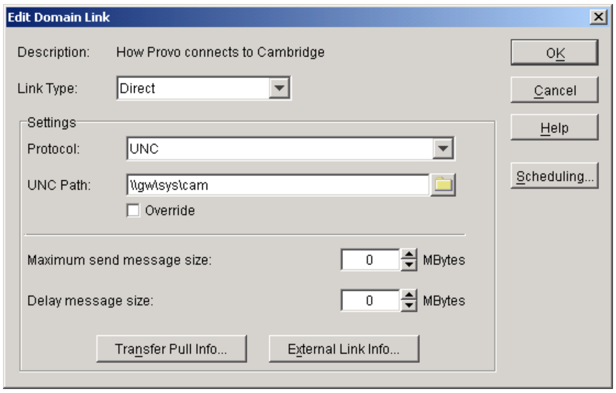
Outbound Links from Provo

Direct	Indirect	Gateway	Undefined
Cambridge San Jose			

Inbound Links to Provo

Direct	Indirect
? San Jose	

2 In the Outbound Links list, double-click the external domain to display the Edit Domain Link dialog box.



Edit Domain Link

Description: How Provo connects to Cambridge

Link Type: Direct

Settings

Protocol: UNC

UNC Path: \\gw\sys\cam

□ Override

Maximum send message size: 0 MBytes

Delay message size: 0 MBytes

3 Modify the following fields:

Link Type: Select Gateway.

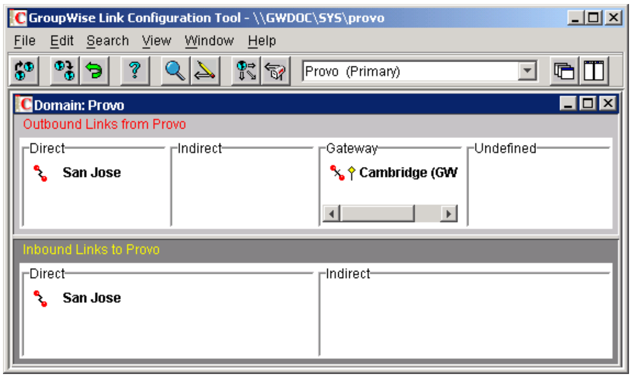
Gateway Link: Select the name of your Internet Agent.

Gateway Access String: Enter the hostname (Internet Agent object > SMTP/MIME tab > Settings page) or foreign ID (Internet Agent object > GroupWise tab > Identification page) assigned to the external domain's Internet Agent (for example, gwia.ctp.com).

Return Link: Leave this set to your Internet Agent domain.

4 Click OK to save your changes.

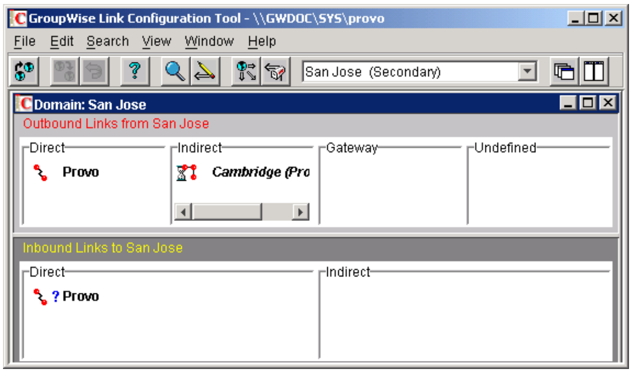
The external domain is displayed in the Gateway column of the Outbound Links list to show that the current domain is using a gateway link to the external domain. The symbol indicates a gateway link. The symbol indicates that the link configuration is not yet saved. To save the configuration information, click the Edit menu > Save.



By default, the rest of the domains in your system should have an indirect link to the external domain. To verify this for a domain:

5 In the list of domains on the Link Configuration utility's toolbar, select the domain whose link you want to check, then verify that the external domain is displayed in the Indirect column of the Outbound Links list.

The ⤷ symbol indicates an indirect link. If the ⧖ symbol is displayed, the link modification has not yet been propagated to the domain.


GroupWise Link Configuration Tool - \\GWDOC\SYS\provo
File Edit Search View Window Help
San Jose (Secondary)
Domain: San Jose
Outbound Links from San Jose
Direct
Provo
Indirect
Cambridge (Pro
Gateway
Undefined
Inbound Links to San Jose
Direct
? Provo
Indirect

6 After verifying your domain links, repeat Step 1 through Step 5 in the second GroupWise system to establish the links to the first GroupWise system. If you do not have administrative rights to that system, you will need to coordinate with that GroupWise system's administrator.

7 Continue with the next section, Checking the Link Status of the External Domain.

Checking the Link Status of the External Domain

The GroupWise MTA has monitoring capabilities that let you determine whether the domains in your system are properly linked to the external domain. When you look at the MTA's operation screen, you should see the external domain added to the domain count in the Status box.

If the link to the external domain is closed, the MTA should be logging and displaying the reasons under its Configuration Status function.

For more information about link protocols, see Chapter 10, "Managing the Links between Domains and Post Offices," on page 131.

Sending Messages Between Systems

After you've established links between the Internet Agent domains in the two GroupWise systems, users in one system can send message to recipients in the other system by including the recipients' fully-qualified GroupWise addresses:

```
userID.post_office.domain or user@host
```

To simplify addressing for your GroupWise users, you can exchange information between the two systems. This enables users in your GroupWise system to use the Address Book when selecting recipients from the other system. For information, see the next section, Exchanging Information Between Systems.

Exchanging Information Between Systems

Exchanging information between two GroupWise systems enables users in either system to use the Address Book when addressing messages to users in the other system. To exchange information, you can choose from the following methods:

External System Synchronization: You can use the External System Synchronization feature to automatically exchange domain, post office, user, resource, and distribution list information between the two systems. After the initial exchange of information, any information that changes in one system is automatically propagated to the other system in order to synchronize the information in that system. This is the recommended method for exchanging information between two systems. For information about setting up synchronization between two external systems, see "External System Synchronization" on page 55.

Manual Creation of Information: You can manually create the other systems' objects (domains, post offices, users, resources, and distribution lists) as external objects in your GroupWise system. When doing so, the names of your external objects need to exactly match the names of the objects as defined in their system. Domains in your system will link to the external domains indirectly through the first external domain you created (this is the external domain that one of your system's domains has a direct link to). The advantage to this method is that you can choose which of the other system's domains, post offices, users, resources, and distribution lists you want included in your system. The disadvantage is that there is a great amount of administrative overhead involved in creating all the objects and, after the objects are created, no automatic synchronization takes place so updates must be made manually.

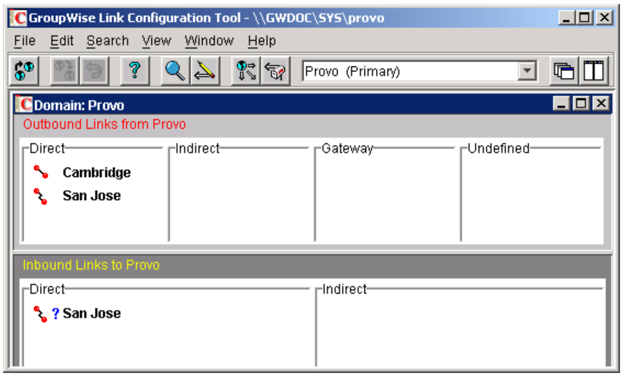
Linking Domains

If you have domains that cannot be linked via a mapped or TCP/IP connection, you can connect them via gateway links, with the Internet Agent defined as the gateway. Both domains being linked must have an Internet Agent installed.

For purposes of reducing confusion in the following steps, the two domains being connected are referred to as Provo and Cambridge. You will need to substitute your domains appropriately.

To configure gateway links between two domains:

1. In ConsoleOne, right-click the Provo domain, click GroupWise Utilities > Link Configuration to display the Link Configuration utility.


GroupWise Link Configuration Tool - \\GWDOC\SYS\provo
File Edit Search View Window Help
Provo (Primary)
Domain: Provo

Outbound Links from Provo

Direct: Cambridge, San Jose

Indirect

Gateway

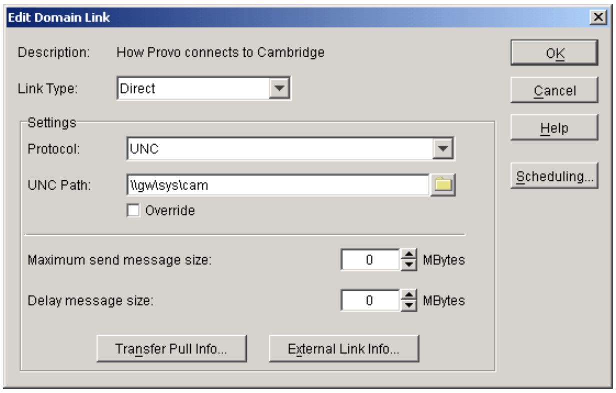
Undefined

Inbound Links to Provo

Direct: ? San Jose

Indirect

2 In the Outbound Links list, double-click the Cambridge domain to display the Edit Domain Link dialog box.



Description: How Provo connects to Cambridge

Link Type: Direct

Protocol: UNC

UNC Path: \\gw\sys\cam

□ Override

Maximum send message size: 0 MBytes

Delay message size: 0 MBytes

3 Modify the following fields:

Link Type: Select Gateway.

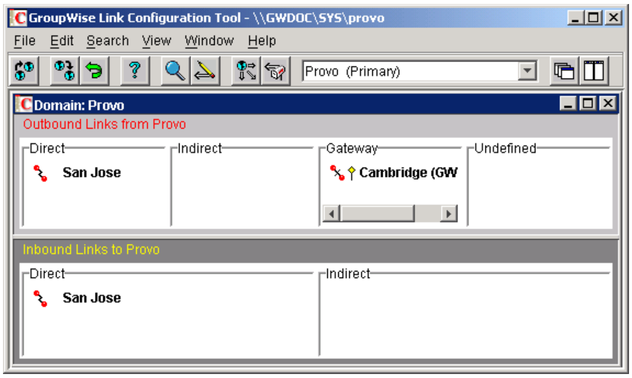
Gateway Link: Select the name of the Provo domain’s Internet Agent.

Gateway Access String: Enter the hostname (Internet Agent object > SMTP/MIME tab > Settings page) or foreign ID (Internet Agent object > GroupWise tab > Identification page) of the Cambridge domain’s Internet Agent (for example, gwia.ctp.com).

Return Link: Leave this set to the Provo domain.

4 Click OK to save your changes.

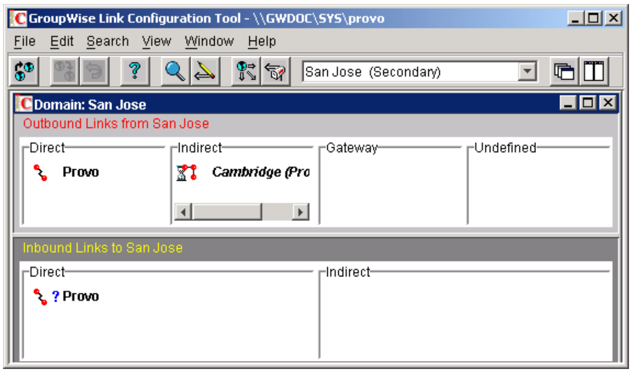
The Cambridge domain is displayed in the Gateway column of the Outbound Links list to show that the Provo domain is using a gateway link to it. The ⤡ symbol indicates a gateway link. The † symbol indicates that the link configuration is not yet saved. To save the configuration information, click the Edit menu > Save.



By default, any domains that are already linked to your Provo domain should have an indirect link to the Cambridge domain through the Provo domain. To verify this for a domain:

5 In the list of domains on the Link Configuration utility's toolbar, select the domain whose link you want to check, then verify that the Cambridge domain is displayed in the Indirect column of the Outbound Links list.

The ↱ symbol indicates an indirect link. If the ⌛ symbol is displayed, the link modification has not yet been propagated to the domain.


GroupWise Link Configuration Tool - \\GWDOC\SYS\provo
File Edit Search View Window Help
San Jose (Secondary)
Domain: San Jose
Outbound Links from San Jose
Direct
Provo
Indirect
Cambridge (Pro
Gateway
Undefined
Inbound Links to San Jose
Direct
? Provo
Indirect

6 After verifying your domain links, repeat Step 1 through Step 5 in the second GroupWise system to establish the links to the first GroupWise system. If you do not have administrative rights to that system, you will need to coordinate with that GroupWise system's administrator.

The GroupWise MTA has monitoring capabilities that let you determine whether the domains in your system are properly linked. When you look at the MTA's operation screen, you should see all domains, regardless of link type, included in the domain count in the Status box.

If the link to a domain is closed, the MTA should be logging and displaying the reasons under its Configuration Status function.

For more information about link protocols, see Chapter 10, "Managing the Links between Domains and Post Offices," on page 131.

56 Using Internet Agent Startup Switches

Startup switches let you modify the way the GroupWise® Internet Agent works. Properly using startup switches can help you fine-tune the Internet Agent for your specific messaging environment.

Choose from the following list to find out how to use Internet Agent startup switches, and for an explanation of the purpose for each of the switches. The switches are grouped into sections according to the features and functionality that they affect. For an alphabetical list of switches, see "Alphabetical List of Switches" on page 767.

- "How to Use Startup Switches" on page 765
- "Required Switches" on page 771
- "Console Switches" on page 772
- "Environment Switches" on page 773
- "SMTP/MIME Switches" on page 775
- "POP3 Switches" on page 792
- "IMAP4 Switches" on page 793
- "HTTP (Web Console) Switches" on page 795
- "SSL Switches" on page 796
- "LDAP Switches" on page 798
- "Log File Switches" on page 800

How to Use Startup Switches

The Internet Agent's primary configuration file is gwia.cfg. At startup or restart, the Internet Agent reads this file for its configuration information. Most Internet Agent startup switches also have corresponding settings in ConsoleOne®.

- "Changing Internet Agent Settings in ConsoleOne" on page 765
- "Modifying the Gwia.cfg File" on page 766
- "Editing Guidelines" on page 766

Changing Internet Agent Settings in ConsoleOne

We recommend that you modify the ConsoleOne setting rather than the gwia.cfg startup switch. If you do modify a gwia.cfg switch, you need to be aware that the switch not only overrides the corresponding ConsoleOne setting but also replaces it.

Modifying the Gwia.cfg File

If you need to change the Internet Agent's configuration and do not have access to ConsoleOne, you can manually edit the gwia.cfg file. Any changes you make to the gwia.cfg file are reflected in ConsoleOne.

The location of the gwia.cfg file used by the Internet Agent depends on the Internet Agent's platform:

- **NetWare:** The gwia.cfg file used by the NetWare® Internet Agent is located in the same directory as the agent (typically sys:\system). Do not edit the gwia.cfg file located in the *domain*\wpgate*gwia* directory; if you do, the changes will not affect the Internet Agent.
- **Linux:** The guia.cfg file used by the Linux Internet Agent is located in the /opt/novell/groupwise/agents/share directory.
- **Windows:** The gwia.cfg file used by the Windows Internet Agent is located in the *domain*\wpgate*gwia* directory. Do not edit the gwia.cfg file located in the same directory as the Internet Agent program. This gwia.cfg file is only used to redirect the Internet Agent to the gwia.cfg file in the *domain*\wpgate*gwia* directory.

Editing Guidelines

If you decide to manually edit the gwia.cfg file, keep the following guidelines in mind when making modifications:

- Archive a copy of the file in case you need to return to the original switch settings.
- Use a text editor to edit the file.
- The comment characters include the semicolon (;), pound sign (#), and asterisk (*), and are used to disable a switch or to add comments. The Internet Agent ignores any line that begins with a comment character.
- Changes made to the configuration file do not take effect until you restart the Internet Agent.
- Switches used in the configuration file must begin with one of the following switch delimiters: / (forward slash) or - (dash). For example, you can use /sd or -sd.
- You can use either a dash (-) or an equals sign (=) to separate a switch from its value. For example, you can use /sd-12 or /sd=12. If you use a dash rather than a forward slash as the switch delimiter, you must use an equal sign (for example, -sd=12).
- None of the switches or switch values are case sensitive. For example, /sd-12 is the same as /SD-12.
- If a switch is specified more than once in the configuration file or on the command line, and if it has a value (such as /ll=normal), only the last instance of the switch will be used.
- The gwia.cfg configuration file is used by default. However, you can also specify another configuration file or use startup switches on the command line when starting the Internet Agent program. If no other configuration file is specified on the command line (using the gwia@*filename* syntax), the default gwia.cfg configuration file will be read and processed before, and in addition to, any command line switches.
- If a configuration file other than gwia.cfg is specified on the command line, the default gwia.cfg configuration file will not be read.

Alphabetical List of Switches

NetWare Internet Agent	Linux Internet Agent	Windows Internet Agent	ConsoleOne Settings
/aql	--aql	/aql	SMTP/MIME > Address Handling > Sender's Address Format
/aqor	--aqor	/aqor	SMTP/MIME > Address Handling > Place Domain and Post Office Qualifiers on Right of Address
/ari	--ari	/ari	N/A
/attachmsg	--attachmsg	/attachmsg	N/A
/badmsg	--badmsg	/badmsg	SMTP/MIME > Undeliverables > Undeliverable or Problem Message
/certfile	--certfile	/certfile	GroupWise > SSL Settings > Certificate File
/cluster	N/A	N/A	N/A
/color	N/A	N/A	N/A
/dbchar822	--dbchar822	/dbchar822	N/A
/dhome	--dhome	/dhome	Server Directories > Settings > SMTP Queues Directory
/defaultcharset	--defaultcharset	/defaultcharset	N/A
/dia	--dia	/dia	SMTP/MIME > Address Handling > Ignore GroupWise Internet Addressing
N/A	N/A	/dialpass	SMTP/MIME > Dial-Up Settings > Password
N/A	N/A	/dialuser	SMTP/MIME > Dial-Up Settings > Username
/displaylastfirst	--displaylastfirst	/displaylastfirst	N/A
/dsn	--dsn	/dsn	SMTP/MIME > ESMTP Settings > Enable Delivery Status Notification (DSN)
/dsnage	--dsnage	/dsnage	SMTP/MIME > ESMTP Settings > DSN Hold Age
/etrnhost	--etrnhost	/etrnhost	SMTP/MIME > Dial-Up Settings > ETRN Host
/etrnqueue	--etrnqueue	/etrnqueue	SMTP/MIME > Dial-Up Settings > ETRN Queue
/fd822	--fd822	/fd822	SMTP/MIME > Address Handling > Non-GroupWIse Domain for RFC-822 Replies
/fdmime	--fdmime	/fdmime	SMTP/MIME > Address Handling > Non-GroupWIse Domain for MIME Replies
/flatfwd	--flatfwd	/flatfwd	N/A
/force7bitout	--force7bitout	/force7bitout	SMTP/MIME > Settings > Use 7 Bit Encoding for All Outbound Messages
/forceinboundauth	--forceinboundauth	/forceinboundauth	N/A

NetWare Internet Agent	Linux Internet Agent	Windows Internet Agent	ConsoleOne Settings
/forceoutboundauth	--forceoutboundauth	/forceoutboundauth	N/A
/fut	--fut	/fut	SMTP/MIME > Undeliverables > Forward Undeliverable Inbound Messages
/group	--group	/group	SMTP/MIME > Address Handling > Expand Groups on Incoming Messages
/help	--help	/help	N/A
/hn	--hn	/hn	N/A
/home	--home	/home	N/A
/httppassword	--httppassword	/httppassword	GroupWise > Optional Gateway Settings > HTTP Password
/httpport	--httpport	/httpport	GroupWise > Network Address > HTTP Port
/httprefresh	--httprefresh	/httprefresh	N/A
/httpssl	--httpssl	/httpssl	GroupWise > Network Address > HTTP SSL
/httpuser	--httpuser	/httpuser	GroupWise > Optional Gateway Settings > HTTP User Name
/imap4	--imap4	/imap4	POP3/IMAP4 > Settings > Enable IMAP4 Service
/imapport	--imapport	/imapport	N/A
/imapsport	--imapsport	/imapsport	N/A
/imapssl	--imapssl	/imapssl	GroupWise > Network Address > IMAP SSL
/ipa	--ipa	/ipa	GroupWise > Network Address > TCP/IP Address Post Office Links tab > Settings
/iso88591is	--iso88591is	/iso88591is	N/A
/it	--it	/it	POP3/IMAP4 > Settings > Number of Threads for IMAP4 Connections
/keyfile	--keyfile	/keyfile	GroupWise > SSL Settings > SSL Key File
/keypasswd	--keypasswd	/keypasswd	GroupWise > SSL Settings > Password
/killthreads	--killthreads	/killthreads	N/A
/koi8	--koi8	/koi8	N/A
/ldap	--ldap	/ldap	LDAP > Settings > Enable LDAP Service
/ldapcntxt	--ldapcntxt	/ldapcntxt	LDAP > Settings > LDAP Context
/ldapipaddr	--ldapipaddr	/ldapipaddr	N/A
/ldapport	--ldapport	/ldapport	N/A
/ldappwd	--ldappwd	/ldappwd	N/A

NetWare Internet Agent	Linux Internet Agent	Windows Internet Agent	ConsoleOne Settings
/ldaprefcntxt	--ldaprefcntxt	/ldaprefcntxt	N/A
/ldaprefurl	--ldaprefurl	/ldaprefurl	LDAP > Settings > LDAP REferral URL
N/A	--ldapserverport	N/A	N/A
/ldapssl	--ldapssl	/ldapssl	N/A
/ldapthrd	--ldapthrd	/ldapthrd	LDAP > Settings > Number of LDAP Threads
/ldapuser	--ldapuser	/ldapuser	N/A
/log	--log	/log	GroupWise > Log Settings > Log File Path
/logdays	--logdays	/logdays	GroupWise > Log Settings > Max Log File Age
/loglevel	--loglevel	/loglevel	GroupWise > Log Settings > Log Level
/logmax	--logmax	/logmax	GroupWise > Log Settings > Max Log Disk Space
/maxdeferhours	--maxdeferhours	/maxdeferhours	SMTP/MIME > Settings > Maximum Number of Hours to Retry a Deferred Message
/mbcount	--mbcount	/mbcount	SMTP/IME > Security Settings > Enable Mailbomb Protection and Mailbomb Threshold
/mbtime	--mbtime	/mbtime	SMTP/IME > Security Settings > Enable Mailbomb Protection and Mailbomb Threshold
/mh	--mh	/mh	SMTP/MIME > Settings > Relay Host for Outbound Messages
/mime	--mime	/mime	SMTP/MIME > Message Formatting > Default Message Encoding: MIME
/mono	N/A	N/A	N/A
/mudas	--mudas	/mudas	SMTP/MIME > Undeliverables > Amount of Original Message to Return to Sender When Message Is Undeliverable
/mv	--mv	/mv	SMTP/MIME > Message Formatting
/nasoq	--nasoq	/nasoq	N/A
/noesmtp	--noesmtp	/noesmtp	N/A
/noiso2022	--noiso2022	/noiso2022	N/A
/nomappriority	--nomappriority	/nomappriority	N/A
/nosmp	N/A	N/A	N/A
/notfamiliar	--notfamiliar	/notfamiliar	N/A
/nqpmt	--nqpmt	/nqpmt	SMTP/MIME > Message Formatting > Enable Quoted Printed Message Text Line Wrapping
/p	--p	/p	SMTP/MIME > Settings > Scan Cycle for Send Directory

NetWare Internet Agent	Linux Internet Agent	Windows Internet Agent	ConsoleOne Settings
/password	N/A	N/A	N/A
/pid	--pid	/pid	N/A
/pop3	--pop3	/pop3	POP3/IMAP4 > Settings > Enable POP3 Service
/popintruderdetect	--popintruderdetect	/popintruderdetect	N/A
/popport	--popport	/popport	N/A
/popsport	--popsport	/popsport	N/A
/popssl	--popssl	/popssl	GroupWise > Network Address > POP SSL
/pt	--pt	--pt	POP3/IMAP4 > Settings > Number of Threads for POP3
/rbl	--rbl	/rbl	Access Control > Blacklists > Blacklist Addresses
/rd	--rd	/rd	SMTP/MIME > Settings > Number of SMTP Receive Threads
/realmailfrom	--realmailfrom	/realmailfrom	N/A
/recv	--recv	/recv	N/A
/rejbs	--rejbs	/rejbs	SMTP/MIME > Security Settings > Reject Mail If Sender's Identity Cannot Be Verified
/rt	--rt	/rt	SMTP/MIME > Message Formatting > Number of Inbound Conversion Threads
/sd	--sd	/sd	SMTP/MIME > Settings > Number of SMTP Send Threads
/send	--send	/send	N/A
N/A	--show	N/A	N/A
/single	--single	/single	N/A
/smp	N/A	N/A	N/A
/smtp	--smtp	/smtp	SMTP-MIME > Settings > Enable SMTP
/smtphome	--smtphome	/smtphome	Server Directories > Settings > Advanced > SMTP Service Queues Directory
N/A	--smtpport	N/A	N/A
/smtpssl	--smtpssl	/smtpssl	GroupWise > Network Address > SMTP SSL
/st	--st	/st	SMTP/MIME > Message Formatting > Number of Outbound Conversion Threads
/tc	--tc	/tc	SMTP/MIME > Timeouts > Commands
/td	--td	/td	SMTP/MIME > Timeouts > Data

NetWare Internet Agent	Linux Internet Agent	Windows Internet Agent	ConsoleOne Settings
/te	--te	/te	SMTP/MIME > Timeouts > Connection Establishment
/tg	--tg	/tg	SMTP/MIME > Timeouts > Greeting
/tr	--tr	/tr	SMTP/MIME > Timeouts > TCP Reset
/tt	--tt	/tt	SMTP/MIME > Timeouts > Connection Termination
/usedialup	--usedialup	/usedialup	SMTP/MIME > Dial-Up Settings > Enable Dial-Up
/user	N/A	N/A	N/A
/uueaa	--uueaa	/uueaa	SMTP/MIME > Message Formatting > UUEncode All Message Attachments
/work	--work	/work	Server Directories > Settings > Conversion Directory
/wrap	--wrap	/wrap	SMTP/MIME > Message Formatting > Line Wrap Length for Message Text on Outbound Mail
/xspam	--xspam	/xspam	N/A

Required Switches

The following switches point the Internet Agent to the Internet Agent's directory. They are assigned their initial value during installation. If you move the Internet Agent to another location, you must update these switches.

/dhome
/hn
/home

The following switches are only for the NetWare version of the GroupWise Internet Agent, and are only required if the Internet Agent is running in remote mode, meaning that it does not reside on the same server as the GroupWise domain directory.

/user
/password

/dhome

Points to the SMTP service work area. This is normally the Internet Agent's gateway directory under the *domain*\wpgate directory. See "Relocating the Internet Agent's Processing Directories" on page 725.

Syntax: `/dhome=`*`pathname`*

NetWare Example: `/dhome=sys:\headq\wpgate\gwia`

Linux Example: `-dhome /gwsystem/provo1/gwia`

Windows Example: `/dhome=c:\gwia`

/hn

Specifies the hostname that is displayed when someone connects to your Internet Agent via a Telnet session. You should enter the hostname assigned to you by your Internet service provider.

Syntax: `/hn=`*`host_name`*

Example: `/hn=gwia.novell.com`

This switch is required only under certain circumstances. Normally, the Internet Agent gets the information from another source and does not need this switch. If you receive a message that the /hn switch is required, you must use the switch. For the NetWare version, the /hn switch is required only if you don't use the hosts file in the sys:\etc directory to indicate the IP address and name of the Internet Agent server. If either of these options (the IP address or the name of the server) is not available, the program cannot start.

/home

Points the Internet Agent to the Internet Agent's gateway directory. This is always a subdirectory of wpgate in the domain directory structure.

Syntax: `/home=`*`gateway_directory`*

NetWare Example: `/home=sys:\headq\wpgate\gwia`

Linux Example: `-home /gwsystem/provo1/gwia`

Windows Example: `/home=j:\headq\wpgate\gwia`

/user (NetWare Only)

Sets the login ID that the NetWare Internet Agent must use to log into a remote file server to access the domain database and Internet Agent directories.

Syntax: `/user-`*`login_ID`*

/password (NetWare Only)

Sets the password that the NetWare Internet Agent must use to log into a remote file server to access the domain database and Internet Agent directories.

Syntax: `/password-`*`password`*

Console Switches

The following switches apply to the Internet Agent console:

/color
/help
/mono
--show

/color

Sets the default color of the Internet Agent console. The values range from 0-7.

Syntax: `color-0|1|2|3|4|5|6|7`

Example: `/color-3`

You can also change the color of the screen for an Internet Agent session. From the menu on the bottom of the console, select Options, then press the key for Colors.

/help

Displays the Help screen for the startup switches.

Syntax: `/help`

Short Syntax: `/h`

/mono

Runs the Internet Agent for a computer with a monochrome monitor.

Syntax: `/mono`

Short Syntax: `/mon`

--show (Linux Only)

Starts the Linux Internet Agent with an agent console interface similar to that provided for the NetWare and Windows Internet Agent. This user interface requires that the X Window System and OpenMotif be running on the Linux server.

Syntax: `--show`

Environment Switches

The following switches configure Internet Agent environment settings such as working directories, NetWare clustering support, and NetWare symmetric multi-processing (SMP).

/ipa
/cluster
/pid
/smp
/nosmp
/smtphome
/work

/ipa

Specifies the IP address (or hostname) of a GroupWise POA that the Internet Agent can use to resolve IP addresses of other post offices in the system. This replaces the need to configure post office links for the Internet Agent in ConsoleOne (Internet Agent object > Post Office Links > Settings).

If you have established a GroupWise name server (ngwnameserver), you can use it. See "Simplifying Client/Server Access with a GroupWise Name Server" on page 449.

Syntax: `/ipa-`*`address`*

Example: `/ipa-ngwnameserver`

/cluster (NetWare Only)

Informs the Internet Agent that it is running in a Novell Cluster Services environment. For detailed information about running the Internet Agent in a clustering environment, see "Implementing the Internet Agent in a Novell Cluster" in "Novell Cluster Services" in the *GroupWise 6.5 Interoperability Guide*.

Syntax: `/cluster`

/pid

Specifies the process ID for this instance of the Internet Agent. You can use the /pid switch to have multiple instances of the Internet Agent running on the same server. The first process is 001. You can use any numbers between 002 and 999 for additional processes.

Syntax: `/pid-`*`number`*

Example: `/pid-002`

/smp (NetWare Only)

Enables the NetWare Internet Agent to use the symmetric multi-processing capability.

Syntax: `/smp`

/nosmp (NetWare Only)

Disables the NetWare Internet Agent's symmetric multi-processing (SMP) capability.

Syntax: `/nosmp`

/smtphome

Specifies a secondary SMTP queues directory for outbound messages. This secondary directory can be helpful for troubleshooting by providing a way to trap messages before they are routed to the Internet. You can also use the secondary directory to run third-party utilities such as a virus scanner on Internet-bound messages. See "Relocating the Internet Agent's Processing Directories" on page 725.

The Internet Agent places all outbound messages in this secondary directory. The messages must then be moved manually (or by another application) to the primary SMTP queue's send directory (/dhome switch) before the Internet Agent will route them to the Internet.

Syntax: `/smtphome`

/work

Sets the directory where the Internet Agent stores its temporary files. On NetWare and Linux, the default work directory is located in the domain, in wpgate\gwia\000.prc\gwwork directory. On Windows, the default work directory *c:\grpwise\gwia* directory, which is not in the domain directory.

Syntax: `/work-pathname`

Short Syntax: `/gw-pathname`

NetWare Example: `/work-sys:\tmp\work`

Linux Example: `-work /opt/novell/groupwise/tmp`

Windows Example: `/work-j:\tmp\work`

/nasoq

By default, the Internet Agent sends the accounting file (acct) to users specified as accountants in ConsoleOne (Internet Agent object > GroupWise > Gateway Administrators). The file is sent daily at midnight and any time the Internet Agent shuts down.

This switch instructs the Internet Agent to send the acct file once daily at midnight, not each time the Internet Agent quits or is shut down.

Syntax: `/nasoq`

SMTP/MIME Switches

The following sections categorize and describe the switches that you can use to configure the Internet Agent's SMTP/MIME settings:

- "SMTP Enabled (/smtp Switch)" on page 775
- "Address Handling" on page 776
- "Message Formatting and Encoding" on page 780
- "Extended SMTP" on page 784
- "Send/Receive Cycle and Threads" on page 784
- "Dial-Up Connections" on page 785
- "Timeouts" on page 786
- "Relay Host" on page 788
- "Host Authentication" on page 788
- "Undeliverable Message Handling" on page 790
- "Mailbomb and Spam Security" on page 790
- "/rbl" on page 791

SMTP Enabled (/smtp Switch)

Enables the Internet Agent to process SMTP messages. See "Configuring Basic SMTP/MIME Settings" on page 661.

Syntax: `/smtp`

Address Handling

The following switches determine how the Internet Agent handles e-mail addresses:

/aql
/aqor
/ari
/dia
/displaylastfirst
/dontreplaceunderscore
/fd822
/fdmime
/group
/keepsendgroups
/killthreads
/msstu
/nomappriority
/notfamiliar
/realmailfrom

/aql

Allows you to determine the address qualification level. It specifies which GroupWise address components (domain.post_office.user) must be included as the user portion of a GroupWise user's outbound Internet address (userhost). Valid options are auto, userid, po, and domain.

This switch is valid only if your system is not configured to use Internet-style addressing, as described in "Internet-Style Addressing" on page 87, or you've configured the Internet Agent to ignore Internet-style addressing, as described in "Configuring How the Internet Agent Handles E-Mail Addresses" on page 664.

Syntax: `/aql-`*`option`*

Example: `/aql-po`

Option	Description
auto	This option causes the gateway to include the addressing components required to make the user's address unique. If a user ID is unique in a GroupWise system, the outbound address uses only the *user_ID*. If the *post_office* or *domain.post_office* components are required to make the address unique, these components are also included in the outbound address. The auto option is the default.
userid	This option requires the gateway to include only the *user_ID* in the outbound Internet address, even if the user ID is not unique in the system. If a recipient replies to a user whose user ID is not unique and no other qualifying information is provided, that reply cannot be delivered.
po	This option requires the gateway to include *post_office.user_ID* in every outbound address, regardless of the uniqueness or non-uniqueness of the user ID.
domain	This option requires the gateway to include the fully-qualified GroupWise address (*domain.post office.user_ID*) in every outbound address, regardless of the uniqueness or non-uniqueness of the user ID. This option guarantees the uniqueness of every outbound Internet address, and ensures that any replies are delivered.

/aqor

The user part of a GroupWise user's outbound Internet address (*user@host*) can and sometimes must include the full Groupwise address (*domain.post_office.user_ID@host*) in order to be unique. The /aqor switch instructs the Internet Agent to move any GroupWise address components, except the *user_ID* component, to the right side of the address following the at sign (@). In this way, GroupWise addressing components become part of the host portion of the outbound Internet address. The /aql switch specifies which components are included.

For example, if the /aqor switch is used (in conjunction with the /aql-domain switch), Bob Thompson's fully qualified Internet address (headquarters.advertising.bob@novell.com) would be resolved to bob@advertising.headquarters.novell.com for all outbound messages.

If the /aqor switch is used with the /aql-po switch, Bob's Internet address would be resolved to bob@advertising.novell.com for all outbound messages.

If you use the /aqor switch to move GroupWise domain or post office names to be part of the host portion on the right side of the address, you must provide a way for the DNS server to identify the GroupWise names. You must either explicitly name all GroupWise post offices and domains in your system as individual MX Records, or you can create an MX Record with wildcard characters to represent all GroupWise post offices and domains. For information about creating MX Records, see details found in RFC #974.

For details about this setting, see "Configuring How the Internet Agent Handles E-Mail Addresses" on page 664.

/ari

Enables or disables additional routing information that is put in the SMTP return address to facilitate replies. This switch might be needed in large systems with external GroupWise domains in which the external GroupWise users have not been configured in your local domain. Options include Never and Always. Most sites do not need to use this switch.

Syntax: `/ari-`*`never`*`|`*`always`*

Example: `/ari-never`

/dia

GroupWise supports both Internet-style addressing (*user@host*) and GroupWise proprietary addressing (*user_ID.post_office.domain*). By default, the Internet Agent uses Internet-style addressing. See "Configuring How the Internet Agent Handles E-Mail Addresses" on page 664.

You can use this switch to disable Internet-style addressing. With Internet-style addressing disabled, messages use the mail domain name in the Foreign ID field in ConsoleOne (Internet Agent object > GroupWise > Identification) for the domain portion of a user's Internet address. The Internet Agent continues to support user and post office aliases in either mode.

Syntax: `/dia`

/displaylastfirst

By default, users' display names are First Name Last Name. If you want users' display names to be Last Name First Name, you can use the /displaylastfirst switch. This forces the display name format to be Last Name First Name, regardless of the preferred address format.

Syntax: `/displaylastfirst`

/dontreplaceunderscore

By default, the Internet Agent accepts addresses of the format:

firstname_lastname@internet_domain_name

even though this is not an address format included in the Allowed Address Formats list in ConsoleOne for configuring Internet addressing, as described in "Allowed Address Formats" on page 91. Use this switch to prevent this address format from being accepted by the Internet Agent.

Syntax: `/dontreplaceunderscore`

/fd822

Specifies a return address for GroupWise replies. A message that has been received by a GroupWise user through the Internet Agent and is replied to has this return address form. These switches cause the Internet Agent to produce a return address of the form *foreign domain.type*:"*user host*." *Foreign domain* can be any foreign domain you have configured and linked to the Internet Agent.

You can use the same foreign domain name for both the /fd822 switch and the /fdmime switch. You can specify multiple foreign domain and kind pairs by placing them in quotes. If multiple foreign domain and kind pairs are used, the first domain/kind pair is the return address for replies to messages received through the Internet Agent. The second domain/kind pair is checked to see what message format is used for old replies in the system. Up to four pairs can be specified with an 80-character limit.

This switch lets you change your foreign domain names in your GroupWise system and still have replies work. For example, if your foreign domain had been called *faraway* and you added a foreign domain called Internet, you could use /fd822-"internet.nonmime smtp.nonmime." This would cause replies to have a return address of internet.nonmime.:"*user@host*." The Internet Agent would also recognize *faraway*. This switch also lets you migrate from one foreign domain to another.

Most administrators do not need to use this switch.

Syntax: `/fd822-`*`foreign_domain.type`*

Example: `/fd822-Internet.nonmime`

/fdmime

Specifies a return address for GroupWise replies. A message that has been received by a GroupWise user through the Internet Agent and is replied to has this return address form. These switches cause the Internet Agent to produce a return address of the form *foreign_domain.type*:"*user host*." *Foreign_domain* can be any foreign domain you have configured and linked to the Internet Agent. *Type* can be either mime or nonmime.

You can use the same foreign domain name for both the /fd822 switch and the /fdmime switch.

You can specify multiple foreign domain and kind pairs by placing them in quotes. If multiple foreign domain and kind pairs are used, the first domain/kind pair is the return address for replies to messages received through the Internet Agent. The second domain/kind pair is checked to see what message format is used for old replies in the system. Up to four pairs can be specified with an 80-character limit.

This switch lets you change your foreign domain names in your GroupWise system and still have replies work. For example, if your foreign domain had been called SMTP and you added a foreign domain called Internet, you could use /fdmime-"internet.mime smtp.mime." This would cause replies to have a return address of internet.mime:"*user@host*." The Internet Agent would also recognize SMTP. This switch also lets you migrate from one foreign domain to another.

Most administrators do not need to use this switch.

Syntax: `/fdmime-foreign_domain.type`

Example: `/fdmime-Internet.mime`

/group

Turns on group expansion. The default startup file has this switch commented out. If it is enabled, an incoming Internet message addressed to a public group is sent to members of that group. See "Configuring How the Internet Agent Handles E-Mail Addresses" on page 664.

Syntax: `/group`

/keepsendgroups

Prevents the Internet Agent from expanding distribution lists on messages going to external Internet users so that the SMTP header does not become too large.

Syntax: `/keepsendgroups`

/killthreads

Instructs the Internet Agent to immediately terminate any active send/receive threads when it restarts.

Syntax: `/killthreads`

/msstu

Instructs the Internet Agent to map spaces to underscores in user addresses for outbound messages. For example, john smith becomes john_smith.

Syntax: `/msstu`

/nomappriority

Disables the function of mapping an x-priority MIME field to a GW priority message.

Syntax: `/nomappriority`

/notfamiliar

Instructs the Internet Agent to not include the user's familiar name, or display name, in the FROM field of the message's MIME header. In other words, the From field will be *address* rather than "*familiar_name*" *address*.

Syntax: `/notfamiliar`

/realmailfrom

Instructs the Internet Agent to use the real user in the Mail From field instead of having auto-forwards come from Postmaster and auto-replies come from Mailer-Daemon.

Syntax: `/realmailfrom`

Message Formatting and Encoding

The following switches determine how the Internet Agent formats and encodes inbound and outbound e-mail messages:

/attachmsg
/dbchar822
/defaultcharset
/force7bitout
/iso88591is
/koi8
/mime
/mv
/noiso2022
/noqpmt
/rt
/st
/uueaa
/wrap

/attachmsg

Instructs the Internet Agent to maintain the original format of any file type attachment.

Syntax: `/attachmsg`

/dbchar822

Instructs the Internet Agent to map inbound non-MIME messages to another character set that you specify. The mapped character set must be an Asian (double-byte) character set.

Syntax: `/dbchar822-`*`charset`*

Example: `/dbchar822-shift_js`

/defaultcharset

Specifies what character set to use if no character set is specified in an incoming message.

Syntax: `/defaultcharset-`*`charset`*

Example: `/defaultcharset-iso-8859-1`

For readability when the character set name includes hyphens (-), you can use an equal sign (=) as the delimiter between the switch and its setting.

Example: `/defaultcharset=iso-8859-1`

/force7bitout

By default, the Internet Agent uses 8-bit MIME encoding for any outbound messages that are HTML-formatted or that contain 8-bit characters. If, after connecting with the receiving SMTP host, the Internet Agent discovers that the receiving SMTP host cannot handle 8-bit MIME encoded messages, the Internet Agent converts the messages to 7-bit encoding.

You can use the /force7bitout switch to force the Internet Agent to use 7-bit encoding and not attempt to use 8 bit MIME encoding. You should use this option if you are using a relay host that does not support 8-bit MIME encoding. See "Configuring Basic SMTP/MIME Settings" on page 661.

Syntax: `/force7bitout`

/iso88591is

Instructs the Internet Agent to map inbound MIME ISO-8859-1 messages to another character set that you specify.

Syntax: `/iso88591is-`*`charset`*

Example: `/iso88591is-big5`

/koi8

Instructs the Internet Agent to map all outbound MIME messages to the KOI8 (Russian) character set.

Syntax: `/koi8`

/mime

Instructs the Internet Agent to send outbound messages in MIME format rather than in RFC-822 format. If you've defined an RFC-822 non-GroupWise domain, as described in "Creating a Non-GroupWise Domain" on page 693, users can still send RFC-822 formatted messages by using the RFC-822 domain in the address string when sending messages. Removing the switch corresponds to enabling the Default Message Encoding: Basic RFC-822 switch in ConsoleOne. See "Determining Format Options for Messages" on page 667.

Syntax: `/mime`

/mv

Specifies a mail view attachment for all inbound Internet messages. A view is the screen that a user sees when a message is opened. This switch helps users identify Internet messages. If you do not specify a view, or if the view has not been configured, the default view is used. See "Protecting Against Unidentified Hosts and Mailbombs (Spam)" on page 668.

Syntax: `/mv-`*`viewname`*

Example: `/mv-Internet`

IMPORTANT: Quotes must surround a mail view name that contains a space (for example, /mv-"Expanded Mail").

How the /mv Switch Works

When the Internet Agent receives an Internet message, it writes the view name you have chosen into a special field of the message. When a user opens that message, the GroupWise client searches the ofviews.ini file for the specified view name. If the client finds the view name and the corresponding view file, it displays the message with that view.

To configure your GroupWise system to use an existing mail view, you must know what the view is named so that you can include it with the /mv switch.

Locating a View

You can identify view files by their .vew extension (for example, usml_1.vew, which is the default). Views are located in the *post_office*\ofviews\win directory. Only views located in this directory are available to users on the post office.

Finding a View's Name

View names are defined in the [Mail] section of the ofviews.ini (and/or ofviewxx.ini) file in the *postoffice*\ofviews\win directory. The ofviews.ini file is an ASCII text file that you can open with any text editor.

The gwia.cfg file that ships with the gateway contains an active /mv-Internet line. If you already have added a system view called Internet, messages that come from the Internet are immediately received with the Internet view you added. Otherwise, use the /mv switch to specify the name of the view you want used.

/noiso2022

Instructs the Internet Agent to not use ISO-2022 character sets. ISO-2022 character sets provide 7-bit encoding for Asian character sets.

Syntax: `/noiso2022`

/nqpmt

Disables quoted printable message text for outbound messages. If this switch is turned on, messages are sent with the Base64 MIME encoding. If you use this switch you need to review the setting for the /wrap switch to ensure that message text wraps correctly. See "Determining Format Options for Messages" on page 667.

Syntax: `/nqpmt`

/rt

Specifies the maximum number of threads that the Internet Agent uses when converting inbound messages from MIME or RFC-822 format to the GroupWise message format. The default setting is 4. See "Determining Format Options for Messages" on page 667.

Multiple threading allows for more than one receive process to be running concurrently. A receive request is assigned to a single thread and is processed by that thread. If you anticipate heavy inbound message traffic, you can increase the number of threads to enhance the speed and performance of the Internet Agent. The number of threads is limited only by the memory resources of your server.

Syntax: `/rt`

/st

Specifies the maximum number of threads that the Internet Agent uses when converting outbound messages from GroupWise message format to MIME or RFC-822 format. The default setting is 4. See "Determining Format Options for Messages" on page 667.

Multiple threading allows for more than one send process to be running concurrently. A send request is assigned to a single thread and is processed by that thread. If you anticipate heavy outbound message traffic, you can increase the number of threads to enhance the speed and performance of the Internet Agent. The number of threads is limited only by the memory resources of your server.

Syntax: /st

/uueaa

Forces the Internet Agent to UUencode any ASCII text files attached to outbound RFC-822 formatted messages. This switch applies only if the /mime switch is not used. Without this switch, the Internet Agent includes the text as part of the message body. See "Determining Format Options for Messages" on page 667.

Syntax: `/uueaa`

/wrap

Sets the line length for outbound messages. This is important if the recipient's e-mail system requires a certain line length. See "Determining Format Options for Messages" on page 667.

Syntax: `/wrap-`*`line_length`*

Example: `/wrap-72`

Forwarded and Deferred Messages

The following switches configure how the Internet Agent handles forwarded and deferred messages:

/flatfwd
/maxdeferhours

/flatfwd

Automatically strips out the empty message that is created when a message is forwarded without adding text, and retains the original sender of the message, rather than showing the user who forwarded it. This facilitates users forwarding messages from GroupWise to other e-mail accounts. Messages arrive in the other accounts showing the original senders, not the users who forwarded the messages from GroupWise.

Syntax: `/flatfwd`

/maxdeferhours

Specifies the number of hours after which the Internet Agent stops trying to send deferred messages. The default is 96 hours, or four days. A deferred message is any message that couldn't be sent because of a temporary problem (host down, MX record not found, and so forth).

For the first hour of the specified time, the Internet Agent tries resending the message every 20 minutes. After the first hour, it tries resending the message every four hours. For example, if you specify 10 hours, the Internet Agent tries resending the message at 20 minutes, 40 minutes, 1 hour, 5 hours, and 9 hours. After the 10 hours has expired, it will return an undeliverable status to the sender. See "Configuring Basic SMTP/MIME Settings" on page 661.

Syntax: `/maxdeferhours`

Extended SMTP

The following switches configure the Internet Agent's Extended SMTP (ESMTP) settings:

/noesmtp
/dsn
/dsnage

/noesmtp

Disables ESMTP support in the Internet Agent.

Syntax: `/noesmtp`

/dsn

Enables Delivery Status Notification (DSN). The Internet Agent will request status notifications for outgoing messages and will supply status notifications for incoming messages. This requires the external e-mail system to also support Delivery Status Notification. Currently, notification consists of two delivery statuses: successful and unsuccessful. See "Using Extended SMTP (ESMTP) Options" on page 663.

Syntax: `/dsn`

/dsnage

The /dsnage switch specifies the number of days that the Internet Agent will retain information about the external sender so that status updates can be delivered to him or her. For example, the default DSN age causes the sender information to be retained for 4 days. If the Internet Agent does not receive delivery status notification from the GroupWise recipient's Post Office Agent (POA) within that time period, it deletes the sender information and the sender does not receive any delivery status notification. See "Using Extended SMTP (ESMTP) Options" on page 663.

Syntax: `/dsnage`

Send/Receive Cycle and Threads

The following switches configure the Internet Agent's SMTP send/receive cycle and threads:

/p
/rd
/sd
/recv
/send
/single
/smtpport

/p

Specifies how often, in seconds, the Internet Agent polls for outbound messages. The default,10 seconds, causes the Internet Agent to poll the outbound message directory every 10 seconds. see "Configuring Basic SMTP/MIME Settings" on page 661.

Syntax: `/p-`*`seconds`*

Example: `/p-5`

/rd

Specifies the maximum number of threads used for processing SMTP receive requests (inbound messages). The default is 16 threads. See "Configuring Basic SMTP/MIME Settings" on page 661.

Syntax: `/rd-`*`number_of_threads`*

Example: `/rd-20`

/sd

Specifies the maximum number of threads used for processing SMTP send requests (outbound messages). The default is 8 threads. See "Configuring Basic SMTP/MIME Settings" on page 661.

Syntax: `/sd-`*`number_of_threads`*

Example: `/sd-12`

/recv

Places the Internet Agent in receive-only mode. If this switch is enabled, the Internet Agent does not send any messages. Use this switch only for troubleshooting.

Syntax: `/recv`

Short Syntax: `/r`

/send

Places the Internet Agent in send-only mode. If you enable this switch, the Internet Agent does not receive any messages. Use this switch only for troubleshooting.

Syntax: `/send`

Short Syntax: `/s`

/single

Instructs the Internet Agent to run one send and receive cycle, then terminate the session. Use this switch only for troubleshooting.

Syntax: `/single`

Short Syntax: `/sc`

--smtpport (Linux only)

Changes the SMTP listen port from the default of 25. Use this switch only if the Internet Agent is receiving messages only from SMTP hosts that can be configured to connect to Internet Agent on a specified port.

Dial-Up Connections

SMTP dial-up services can be used when you don't require a permanent connection to the Internet and want to periodically check for mail messages queued for processing. The following switches can be used when configuring dial-up services. For more information about dial-up services, see "Configuring SMTP Dial-Up Services" on page 671.

/usedialup
/etrnhost
/etrnqueue
/dialuser
/dialpass

/usedialup

Enables SMTP dial-up services. See "Enabling Dial-Up Services" on page 671.

Syntax: `/usedialup`

/etrnhost

Specifies the IP address or DNS hostname of the mail server (where your mail account resides) at your Internet Service Provider. You should obtain this address from your Internet Service Provider. See "Enabling Dial-Up Services" on page 671.

Syntax: `/etrnhost-`*`address`*

Example: `/etrnhost-172.16.5.18`

/etrnqueue

Specifies your e-mail domain as provided by your Internet Service Provider. See "Enabling Dial-Up Services" on page 671.

Syntax: `/etrnqueue-`*`email_domain`*

Example: `/etrnqueue-novell.com`

/dialuser (Windows Only)

Specifies the RAS Security user if you are using a Windows NT Remote Access Server (RAS) and the Internet Agent is not running on the same server as the RAS.

Syntax: `/dialuser-`*`username`*

Example: `/dialuser-rasuser`

/dialpass (Windows Only)

Specifies the RAS Security user's password if you are using a Windows NT Remote Access Server (RAS) and the Internet Agent is not running on the same server as the RAS.

Syntax: `/dialpass-`*`password`*

Example: `/dialpass-raspassword`

Timeouts

The following switches specify how long SMTP services waits to receive data that it can process. After the time expires, the Internet Agent might give a TCP read/write error. Leave these switches at the default setting unless you are experiencing a problem with communication.

/tc
/td

/te

/tg

/tr

/tt

/tc

Specifies how long the program waits for an SMTP command. The default is 2 minutes.

Syntax: `/tc-`*`minutes`*

Example: `/tc-3`

/td

Specifies how long the program waits for data from the receiving host. The default is 5 minutes.

Syntax: `/td-`*`minutes`*

Example: `/td-2`

/te

Specifies how long the program waits for the receiving host to establish a connection. The default is 5 minutes.

Syntax: `/te-`*`minutes`*

Example: `/te-2`

/tg

Specifies how long the program waits for the initial greeting from the receiving host. The default is 3 minutes.

Syntax: `/tg-`*`minutes`*

Example: `/tg-2`

/tr

Specifies how long the program waits for a TCP read. The default is 10 minutes.

Syntax: `/tr-`*`minutes`*

Example: `/tr-2`

/tt

Specifies how long the program waits for the receiving host to terminate the connection. The default is 5 minutes.

Syntax: `/tt-`*`minutes`*

Example: `/tt-2`

Relay Host

The following switch configures whether or not the Internet Agent uses a relay host.

/mh

/mh

Specifies the IP address or DNS hostname of a relay host that you want the Internet Agent to use for outbound messages. The relay host can be part of your network or can reside at the Internet service provider's site. This switch is typically used in firewall integration if you want one server, the specified relay host, to route all mail. See "Configuring Basic SMTP/MIME Settings" on page 661.

Syntax: `/mh-`*`address`*

Example: `/mh-151.155.111.11`

Host Authentication

The Internet Agent supports SMTP host authentication for both inbound and outbound message traffic.The following switches are used with inbound and outbound authentication:

/forceinboundauth
/forceoutbountauth

/forceinboundauth

Ensures that the Internet Agent accepts messages only from remote SMTP hosts that use the AUTH LOGIN authentication method to provide a valid GroupWise user ID and password. The remote SMTP hosts can use any valid GroupWise user ID and password. However, for security reasons, we recommend that you create a dedicated GroupWise user account for remote SMTP host authentication.

Syntax: `/forceinboundauth`

/forceoutboundauth

Ensures that the Internet Agent sends messages only to remote SMTP hosts that are included in a gwauth.cfg text file. The remote SMTP hosts must support the AUTH LOGIN authentication method.

The gwauth.cfg file must reside in the *domain*\wpgate*gwia* directory and use the following format:

```
domain_name authuser authpassword
```

For example:

```
smtp.novell.com remotehost novell
```

You can define multiple hosts in the file. Make sure you include a hard return after the last entry.

If you use this switch, you need to include your Internet Agent as an entry in the gwauth.cfg file to enable status messages to be returned to GroupWise users. You can use any GroupWise user ID and password for your Internet Agent's authentication credentials. However, for security reasons, we recommend that you create a dedicated GroupWise user account for your Internet Agent.

Syntax: `/forceoutboundauth`

Undeliverable Message Handling

The following switches determine how the Internet Agent handles undeliverable messages:

/badmsg
/fut
/mudas

/badmsg

Specifies where to send problem messages. Problem messages can be placed in the Internet Agent problem directory (gwprob), they can be sent to the postmaster, or they can be sent to both or neither. The values for this switch are move, send, both, and neither.

The move option specifies to place problem messages in the gwprob directory for the Internet Agent. The send option specifies to send the message as an attachment to the Internet Agent postmaster defined in ConsoleOne (Internet Agent object > GroupWise > Gateway Administrators). The both option specifies to move the message to gwprob and send it to the postmaster. The neither option specifies to discard problem messages. The default when no switch is specified is move. See "Determining What to Do with Undeliverable Messages" on page 670.

Syntax: `/badmsg-move|send|both|neither`

Example: `/badmsg-both`

/fut

Forwards undeliverable messages to the host specified. This can be useful if you use UNIX sendmail aliases. See "Determining What to Do with Undeliverable Messages" on page 670.

Syntax: `/fut-`*`host`*

Example: `/fut-novell.com`

/mudas

Controls how much of the original message is sent back when a message is undeliverable. By default, only 2 KB of the original message are sent back. The value is specified in KB (8=8KB). See "Determining What to Do with Undeliverable Messages" on page 670.

Syntax: `/mudas-`*`KB`*

Example: `/mudas-16`

Mailbomb and Spam Security

Multiple unsolicited messages (sometimes called a *mailbomb* or *spam*) from the Internet can potentially harm your GroupWise messaging environment. At the least, it can be annoying to your users. You can use the following switches to help protect your GroupWise system from malicious, accidental, and annoying attacks:

/mbcount
/mbtime
/rejbs
/xspam
/rbl

/mbcount

Sets the number of messages that can be received from a single IP address in a given number of seconds before the Internet Agent denies access to its GroupWise system. It provides a form of system security to protect your system from mailbombs.

For example, with /mbcount set to 25 and /mbtime set to 60 seconds, if these limits are exceeded the sender's IP address are blocked from sending any more messages. The IP address of the sender is also displayed in the Internet Agent console. You can permanently restrict access to your system by that IP address through settings on the Access Control page in ConsoleOne (Internet Agent object > Access Control). By default, the mailbomb feature is turned off. To enable this feature, you must specify a value for mailbomb count and mailbomb time. See "Protecting Against Unidentified Hosts and Mailbombs (Spam)" on page 668.

Syntax: `/mbcount-`*number*

Example: `/mbcount-25`

/mbtime

Specifies the mailbomb time limit in seconds. This switch works with the /mbcount switch to block access to your GroupWise system from unsolicited inundations of e-mail. The default value is 10 seconds. See "Protecting Against Unidentified Hosts and Mailbombs (Spam)" on page 668.

Syntax: `/mbtime-`*seconds*

Example: `/mbtime-60`

/rejbs

Prevents delivery of messages if the sender's host is not authentic. When this switch is used, the Internet Agent refuses messages from a host if a DNS reverse lookup shows that a PTR record does not exist for the IP address of the sender's host. See "Protecting Against Unidentified Hosts and Mailbombs (Spam)" on page 668.

If this switch is not used, the Internet Agent accepts messages from any host, but displays a warning if the initiating host is not authentic.

Syntax: `/rejbs`

/xspam

Flags messages to be handled by the client Junk Mail Handling feature if they contain an x-spamflag=yes in the MIME header.

/rbl

Lets you define the addresses of blacklist sites (free or fee-based) you want the Internet Agent to check for blacklisted hosts. If a host is included in a site's blacklist, the Internet Agent does not accept messages from it.

Syntax: `/rbl-blackholes.mail-abuse.org,relays.ordb.org,bl.spamcop.net`

This switch corresponds to the Blacklist Addresses list (Internet Agent object > Access Control tab > Blacklists page). For details about this setting, see "Real-Time Blacklists" on page 719.

POP3 Switches

There are five optional startup switches that can be used to configure the Internet Agent's POP3 service:

/pop3
/popintruderdetect
/popport
/popsport
/popssl
/pt

/pop3

Enables POP3 client access to GroupWise mailboxes through the Internet Agent. See "Enabling POP3/IMAP4 Services" on page 684.

Syntax: `/pop3`

/popintruderdetect

Instructs the Internet Agent to log POP e-mail clients in through the POA so that the POA's intruder detection can take effect, if intruder has been configured in ConsoleOne (POA object > Client Access Settings > Intruder Detection). This switch cannot be used with older POAs that do not support intruder detection.

Syntax: `/popintruderdetect`

/popport

By default, the Internet Agent listens for POP3 connections on port 110. This switch allows you to change the POP3 listen port.

Syntax: `/popport-`*`port_number`*

Example: `/popport-111`

/popsport

By default, the Internet Agent listens for secure (SSL) POP3 connections on port 995. This switch allows you to change the POP3 SSL listen port.

Syntax: `/popsport-`*`port_number`*

Example: `/popsport-996`

/popssl

Disables, enables, or requires secure (SSL) connections between POP3 clients and the Internet Agent. See "Securing Internet Agent Connections Via SSL" on page 753.

Syntax: `/popssl-`*`enabled|disabled|required`*

Example: `/popssl-required`

Option	Description
enabled	The POP3 client determines whether an SSL connection or non-SSL connection is used. By default, the Internet Agent listens for SSL connections on port 995 and non-SSL connections on port 110. You can use the /popsport and /popport switches to change these ports.
required	The Internet Agent forces SSL connections on port 995 and port 110. Non-SSL connections are denied. You can use the /popsport and /popport switches to change these ports.
disabled	The Internet Agent listens for connections only on port 110, and the connections are not secure. You can use the /popport switch to change this port.

/pt

Specifies the maximum number of threads to be used for POP3 connections. The default number is 10. You are limited only by the memory resources of your server. See "Enabling POP3/IMAP4 Services" on page 684.

Syntax: `/pt-*number_of_threads*`

Example: `/pt-15`

IMAP4 Switches

There are five optional startup switches that can be used to configure the Internet Agent's IMAP4 service:

/imap4
/imapport
/imapreadlimit
/imapsport
/imapssl
/it

/imap4

Enables IMAP4 client access to GroupWise mailboxes through the Internet Agent. See "Enabling POP3/IMAP4 Services" on page 684.

Syntax: `/imap4`

/imapport

By default, the Internet Agent listens for IMAP4 connections on port 143. This switch allows you to change the IMAP4 listen port.

Syntax: `/imapport-*port_number*`

Example: `/imapport-144`

/imapreadlimit

By default, the Internet Agent downloads a maximum of 5,000 items at a time. This switch allows you to specify, in thousands, the maximum number of items you want the Internet Agent to download. For example, specifying 10 indicates 10,000.

Syntax: `/imapreadlimit`

Example: `/imapreadlimit-20`

/imapsport

By default, the Internet Agent listens for secure (SSL) IMAP4 connections on port 993. This switch allows you to change the IMAP4 SSL listen port.

Syntax: `/imapsport-`*`port_number`*

Example: `/imapsport-994`

/imapssl

Disables, enables, or requires secure (SSL) connections between IMAP4 clients and the Internet Agent. See "Securing Internet Agent Connections Via SSL" on page 753.

Syntax: `/IMAP4ssl-`*`enabled|disabled|required`*

Example: `/popssl-required`

Option	Description
enabled	The IMAP4 client determines whether an SSL connection or non-SSL connection is used. By default, the Internet Agent listens for SSL connections on port 993 and non-SSL connections on port 143. You can use the /imapsport and /imapport switches to change these ports.
required	The Internet Agent forces SSL connections on port 993 and port 143. Non-SSL connections are denied. You can use the /imapsport and /imapport switches to change these ports.
disabled	The Internet Agent listens for connections only on port 143, and the connections are not secure. You can use the /imapport switch to change this port.

/it

Specifies the maximum number of threads to be used for IMAP4 connections. The default number is 10. You are limited only by the memory resources of your server. See "Enabling POP3/IMAP4 Services" on page 684.

Syntax: `/it-`*`number_of_threads`*

Example: `/it-15`

HTTP (Web Console) Switches

The following switches enable the HTTP Web console and control its configuration settings. The Web console enables you to monitor the Internet Agent through a Web browser. For more information, see "Monitoring the Internet Agent through the Web Console" on page 742.

/httpport
/httpuser
/httppassword
/httprefresh
/httpssl

/httpport

Specifies the port where the Internet Agent listens for the Web console. The default port established during installation is 9850.

Syntax: `/httpport-port_number`

Example: `/httpport-9851`

/httpuser

By default, any user who knows the Internet Agent's address and port (/httpport) can use the Web console. This switch adds security to the Web console by forcing users to log into the Web console using the specified username. The /httppassword switch must also be used to establish the user password.

Syntax: `/httpuser-username`

Example: `/httpuser-gwia`

The *username* can be any arbitrary name.

/httppassword

Specifies the password that must be supplied along with the username provided by /httpuser.

Syntax: `/httppassword-password`

Example: `/httppassword-monitor`

/httprefresh

By default, the Internet Agent refreshes the Web console information every 60 seconds. You can use this switch to override the default refresh interval.

Syntax: `/httprefresh-seconds`

Example: `/httprefresh-120`

/httpssl

Enables the Internet Agent to use a secure connection to a Web browser being used to display the Internet Agent Web console. The Web browser must also be enabled to use SSL; if it is not, a non-secure connection is used. See "Securing Internet Agent Connections Via SSL" on page 753.

Syntax: `/httpssl`

SSL Switches

The Internet Agent can use SSL to enable secure SMTP, POP, IMAP, and HTTP connections. The following switches can be used to 1) specify the server certificate file, key file, and key file password required for SSL and 2) enable or disable SSL for SMTP, POP, IMAP, and HTTP connections. See "Securing Internet Agent Connections Via SSL" on page 753.

/certfile
/keyfile
/keypasswd
/smtpssl
/httpssl
/popssl
/imapssl
/ldapssl

/certfile

Specifies the server certificate file to use. The file must be in Base64/PEM or PFX format. If the file is not in the same directory as the Internet Agent program, specify the full path.

Syntax: `/certfile-`*`filename`*

Example: `/certfile-\\server1\sys\server1.crt`

/keyfile

Specifies the private key file to use. The key file is required if the certificate file does not contain the key. If the certificate file contains the key, do not use this switch. When specifying a filename, use the full path if the file is not in the same directory as the Internet Agent program.

Syntax: `/keyfile-`*`filename`*

Example: `/keyfile-\\server1\sys\server1.key`

/keypasswd

Specifies the private key password. If the key does not require a password, do not use this switch.

Syntax: `/keypasswd-`*`password`*

Example: `/keypasswd-novell`

/smtppssl

Enables the Internet Agent to use a secure connection to other SMTP hosts. The SMTP host must also be enabled to use SSL or TLS (Transport Layer Security); if it is not, a non-secure connection is used.

Syntax: `/smtppssl`

/httpssl

Enables the Internet Agent to use a secure connection to a Web browser being used to display the Internet Agent Web console. The Web browser must also be enabled to use SSL; if it is not, a non-secure connection is used.

Syntax: `/httpssl`

/popssl

Disables, enables, or requires secure (SSL) connections between POP3 clients and the Internet Agent.

Syntax: `/popssl-`*`enabled|disabled|required`*

Example: `/popssl-required`

Option	Description
enabled	The POP3 client determines whether an SSL connection or non-SSL connection is used. By default, the Internet Agent listens for SSL connections on port 995 and non-SSL connections on port 110. You can use the /popsport and /popport switches to change these ports.
required	The Internet Agent forces SSL connections on port 995 and port 110. Non-SSL connections are denied. You can use the /popsport and /popport switches to change these ports.
disabled	The Internet Agent listens for connections only on port 110, and the connections are not secure. You can use the /popport switch to change this port.

/imapssl

Disables, enables, or requires secure (SSL) connections between IMAP4 clients and the Internet Agent.

Syntax: `/IMAP4ssl-`*`enabled|disabled|required`*

Example: `/popssl-required`

Option	Description
enabled	The IMAP4 client determines whether an SSL connection or non-SSL connection is used. By default, the Internet Agent listens for SSL connections on port 993 and non-SSL connections on port 143. You can use the /imapsport and /imapport switches to change these ports.

Option	Description
required	The Internet Agent forces SSL connections on port 993 and port 143. Non-SSL connections are denied. You can use the /imapsport and /imapport switches to change these ports.
disabled	The Internet Agent listens for connections only on port 143, and the connections are not secure. You can use the /imapport switch to change this port.

/ldapssl

Instructs the Internet Agent to use a secure (SSL) connection with an LDAP server. For more information about why the Internet Agent would need to connect to an LDAP server, see "LDAP Switches" on page 798

Syntax: `/ldapssl`

LDAP Switches

The Internet Agent can perform GroupWise authentication of POP3/IMAP4 clients through an LDAP server and can also perform LDAP queries for GroupWise information. see "Enabling LDAP Services" on page 682.

The following sections describe the switches required to configure this functionality:

- "GroupWise Authentication Switches" on page 798
- "LDAP Query Switches" on page 799

GroupWise Authentication Switches

When a POP3/IMAP4 user attempts to access a GroupWise mailbox on a post office that has been configured for LDAP authentication, the Internet Agent connects to the post office's POA, which then connects to the LDAP server so that the LDAP server can authenticate the user.

This process works automatically provided that the Internet Agent's link to the post office is client/server (meaning that it communicates through TCP/IP to the post office's POA). If the Internet Agent is using a direct link to the post office directory rather than a client/server link to the post office's POA, the Internet Agent must communicate directly with the LDAP server rather communicate through the POA.

The following switches are used to provide the Internet Agent with the required LDAP server information:

/ldapipaddr
/ldapport
/ldapssl
/ldapuser
/ldappwd

/ldapipaddr

Specifies the IP address of the LDAP server through which GroupWise authentication takes place.

Syntax: `/ldapipaddr-`*`address`*

Example: `/ldapipaddr-123.456.78.90`

/ldapport

Specifies the port number being used by the LDAP server. The standard non-SSL LDAP port number is 389. The standard SSL LDAP port number is 636.

Syntax: `/ldapport-`*`number`*

Example: `/ldapport-389`

/ldapssl

Instructs the Internet Agent to use a secure (SSL) connection with the LDAP server.

Syntax: `/ldapssl`

/ldapuser

Specifies a user that has rights to the LDAP directory. The user must have at least Read rights.

Syntax: `/ldapuser-`*`username`*

Example: `/ldapuser-ldap`

/ldappwd

Specifies the password of the user specified by the /ldapuser switch.

Syntax: `/ldapuser-`*`username`*

Example: `/ldapuser-ldap`

LDAP Query Switches

The Internet Agent can function as an LDAP server, allowing LDAP queries for GroupWise user information contained in the directory. The following switches configure the Internet Agent as an LDAP server.

/ldap
/ldapthrd
/ldapcntxt
/ldaprefurl
/ldaprefcntxt
/ldapserverport

/ldap

Enables the Internet Agent as an LDAP server.

Syntax: `/ldap`

/ldapthrd

Specifies the maximum number of threads the Internet Agent can use for processing LDAP queries. The default is 10.

Syntax: `/ldapthrd-`*`number`*

Example: `/ldapthrd-5`

/ldapcntxt

Limits the directory context in which the LDAP server searches. For example, you could limit LDAP searches to a single Novell organization container located under the United States country container.

If you restrict the LDAP context, you must make sure that users, when defining the directory in their e-mail client, enter the same context (using the identical text you did) in the Search Base or Search Root field.

Syntax: `/ldapcntxt-"`*`context`*`"`

Example: `/ldapcntxt-"O=Novell,C=US"`

/ldaprefurl

Defines a secondary LDAP server to which you can refer an LDAP query if the query fails to find a user or address in your GroupWise system. For this option to work, the requesting Web browser must be able to track referral URLs.

Syntax: `/ldaprefurl-`*`url`*

Example: `/ldapurl-ldap://ldap.provider.com`

/ldaprefcntxt

Limits the directory context in which the secondary (referral) LDAP server searches.

Syntax: `/ldaprefcntxt-"`*`context`*`"`

Example: `/ldaprefcntxt-"O=Novell,C=US"`

--ldapserverport (Linux Only)

Used to change the LDAP listen port from the default of 389.

Log File Switches

The following switches control how the Internet Agent uses the log file. The log file keeps a record of all Internet Agent activity. See "Using Internet Agent Log Files" on page 746.

/log
/logdays
/loglevel
/logmax

/log

On NetWare and Windows, the log files are stored in the *domain*\wpgate*gwia*\000.prc directory by default. On Linux, they are stored in /var/log/novell/groupwise/*domain_name*.gwia by default. The log files are named after the month, day, and log number for that date (*mmdd*gwia.*nn*).You can use the /log switch to redirect the log files to a different location.

Syntax: `/log-`*`log_file_directory`*

Short Syntax: `/pl-`*`log_file_directory`*

NetWare Example: `/log-sys:\log\gwia`

Linux Example: `--log /opt/novell/groupwise/agents/log`

Windows Example: `/log-c:\log\gwia`

/logdays

By default, log files are deleted after 7 days.This switch overrides the default setting. The range is from 1 to 360 days.

Syntax: `/logdays-`*`days`*

Short Syntax: `/lt-`*`days`*

Example: `/logdays-5`

/loglevel

Defines the amount of information to record in log files.

The values are:

- Diag
- Verbose
- Normal (Default)
- Off

Syntax: `/loglevel-`*`level`*

Short Syntax: `/ll-`*`level`*

Example: `/loglevel-verbose`

/logmax

Controls the maximum amount of disk space for all log files. The amount of disk space each log file consumes is added together to determine the total amount of disk space used. When the limit is reached, the Internet Agent overwrites the existing log files, starting with the oldest one. The default is 1 MB. The range is from 256 KB to unlimited size. Use 0 for unlimited disk space.

Syntax: `/logmax-`*`KB`*

Short Syntax: `/ls-`*`KB`*

Example: `/logmax-512`

XII WebAccess

57 Scaling WebAccess

If your GroupWise® system is relatively small (one domain and a few post offices) and all post offices reside in the same location, a basic installation of GroupWise WebAccess might very well meet your needs. However, if your GroupWise system is large, spans multiple locations, or requires failover support, you might need to scale your GroupWise WebAccess installation to better meet the reliability, performance, and availability needs of your users.

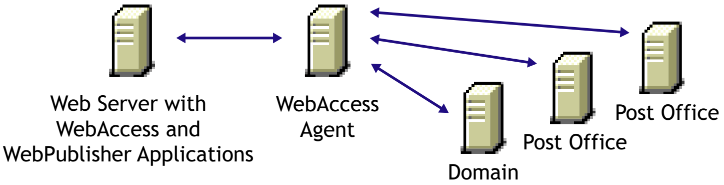
The following sections provide information about the various configurations you can implement and instructions to help you create the configuration you choose:

- "WebAccess Configurations" on page 805
- "Installing Additional WebAccess Components" on page 807
- "Configuring Redirection and Failover Support" on page 810

For information about creating a basic GroupWise WebAccess installation, see "Installing GroupWise WebAccess" in the *GroupWise 6.5 Installation Guide*.

WebAccess Configurations

A basic installation of GroupWise WebAccess requires the WebAccess Agent and the WebAccess Application, as shown in the following diagram. The WebPublisher Application is also required if you plan to use GroupWise WebPublisher.

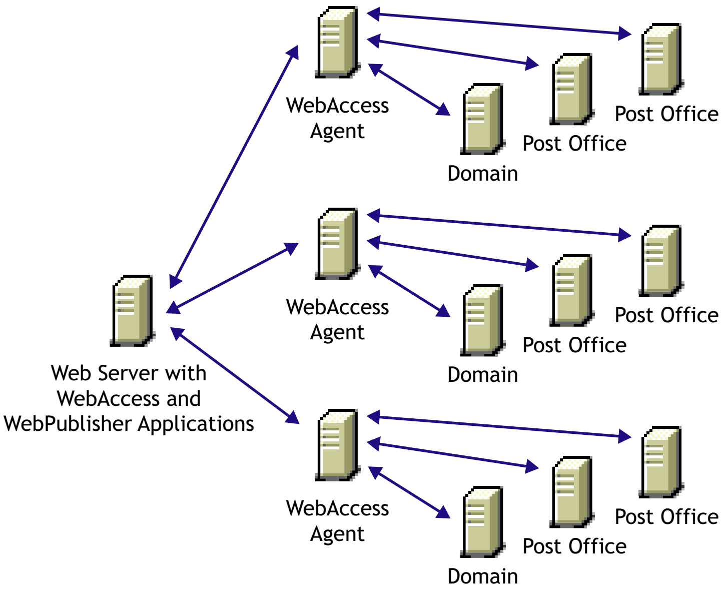


Depending on your needs, it might be necessary for you to add additional WebAccess Agents or to have multiple Web servers running the WebAccess Application and WebPublisher Application.

- "Multiple WebAccess Agents" on page 805
- "Multiple WebAccess and WebPublisher Applications" on page 806

Multiple WebAccess Agents

GroupWise WebAccess is designed to allow one installation of the WebAccess Application and WebPublisher Application to support multiple WebAccess Agents, as shown in the following diagram.

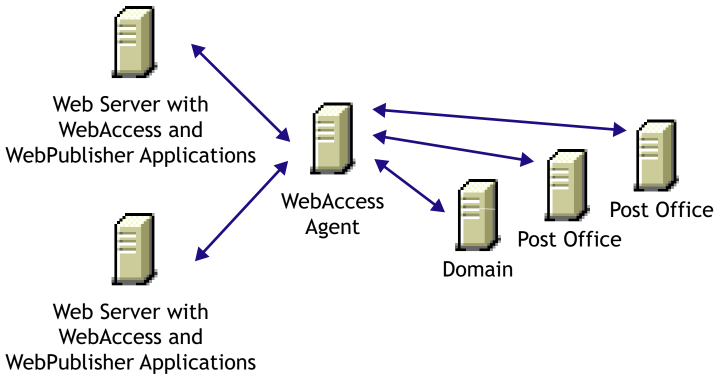


There are various reasons why you might want to add additional WebAccess Agents, including:

- **Improving reliability:** One WebAccess Agent might provide sufficient access and performance, but you want to protect against downtime that would occur if the WebAccess Agent became unavailable due to server failure or some other reason. Installing more than one WebAccess Agent enables you to set up failover support to make your system more reliable.
- **Improving performance:** The WebAccess Agent is designed to be close to the GroupWise databases. It requires direct access to a domain database and either direct access to post office databases or TCP/IP access to the Post Office Agents. For best performance, you should ensure that the WebAccess Agent is on the same local area network as the domain and post offices it needs access to. For example, in most cases you would not want a WebAccess Agent in Los Angeles accessing a post office in London.
- **Improving availability:** The WebAccess Agent has 12 threads assigned to process user requests, which means that it can process only 12 requests at one time regardless of the number of users logged in. If necessary, you can increase the number of threads allocated to the WebAccess Agent, but each thread requires additional server memory. If you reach a point where WebAccess is unavailable to users because thread utilization is at a peak and all server memory is being used, you might need to have several WebAccess Agents, installed on different network servers, servicing your post offices. For information about changing the number of allocated threads, see "Configuring the WebAccess Agent" on page 829.

Multiple WebAccess and WebPublisher Applications

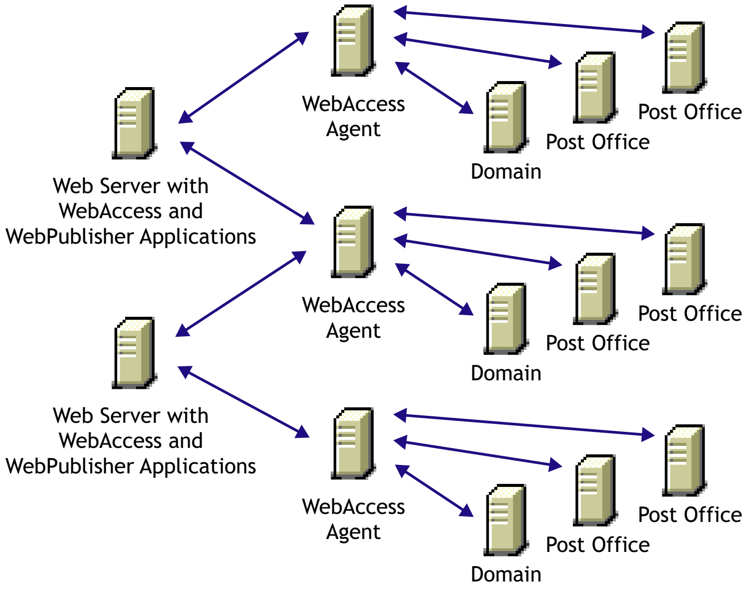
As with the WebAccess Agent, you can also install the WebAccess Application and WebPublisher Application to multiple Web servers, as shown in the following diagram.



Some reasons for wanting to use this type of configuration include:

- Enabling WebAccess users on an intranet to access GroupWise through an internal Web server and WebAccess users on the Internet to access GroupWise through an exposed Web server.
- Increasing Web server performance by balancing the workload among several Web servers, especially if you are using the Web server for other purposes in addition to GroupWise WebAccess.
- Hosting WebAccess (the WebAccess Application) on one Web server for your GroupWise users and WebPublisher (the WebPublisher Application) on another Web server for public Internet use.

If necessary, you can use multiple WebAccess Agents in this configuration, as shown below.



Installing Additional WebAccess Components

The following sections assume that you have installed at least one WebAccess Agent and one WebAccess Application (or WebPublisher Application) and now need to install additional agents or applications.

- "Installing Additional Components on NetWare or Windows" on page 808
- "Installing Additional Components on Linux" on page 809

Installing Additional Components on NetWare or Windows

- "Installing a NetWare or Windows WebAccess Agent" on page 808
- "Installing a NetWare or Windows WebAccess or WebPublisher Application" on page 808

For more information, see "Setting Up GroupWise WebAccess on NetWare or Windows" in the *GroupWise 6.5 Installation Guide*.

Installing a NetWare or Windows WebAccess Agent

1 Insert the *GroupWise 6.5 Administrator* CD into the CD drive to start the Installation program, click Install Products, click GroupWise WebAccess, then click Install GroupWise WebAccess. If the Installation program does not start automatically, run setup.exe from the root of the CD.

   or

   If you've already copied the GroupWise WebAccess software to a software distribution directory, run setup.exe from the internet\webacces directory.

2 Click Yes to accept the license agreement and display the Select Components dialog box.

3 Deselect all components except the GroupWise WebAccess Agent, then click Next.

4 Follow the prompts to create the WebAccess Agent's gateway directory, install the WebAccess Agent software, and create the WebAccess Agent's object in Novell® eDirectory™.

   If you are installing to a domain where another WebAccess Agent already exists, you must use a different directory and object name than the one used for the existing WebAccess Agent.

5 When installation is complete, you will need to configure your system so that the WebAccess and WebPublisher Applications know about the WebAccess Agent and can direct the appropriate user requests to it. For information, see "Configuring Redirection and Failover Support" on page 810.

Installing a NetWare or Windows WebAccess or WebPublisher Application

To install a WebAccess Application or a WebPublisher Application to a web server:

1 Insert the *GroupWise Administrator* CD into the CD drive to start the installation program, click Install Products, click Groupwise WebAccess, then click Install GroupWise WebAccess. If the installation program does not start automatically, run setup.exe from the root of the CD.

   or

   If you've already copied the Groupwise WebAccess software to a software distribution directory, run setup.exe from the internet/webacces directory.

2 Click Yes to accept the license agreement and display the Select Components dialog box.

3 Deselect all components except the GroupWise WebAccess application and/or the Groupwise WebPublisher Application, then click Next.

   The WebAccess Application and WebPublisher Application must be associated with a WebAccess Agent. For information on configuring a WebAccess or WebPublisher Application to connect to other WebAccess Agents, see "Configuring Redirection and Failover Support" on page 810.

4 Enter the path for the WebAccess Agent's gateway directory.

5 Follow the prompts to install the files to the web server. Restart the Web server.

Installing Additional Components on Linux

- "Installing a Linux WebAccess Agent" on page 809
- "Installing a Linux WebAccess and WebPublisher Application" on page 809

For more information, see "Setting Up GroupWise WebAccess on Linux" in the *GroupWise 6.5 Installation Guide*.

Installing a Linux WebAccess Agent

1. Make sure that LDAP is running on your eDirectory server and that it is configured to accept login from the WebAccess Agent Installation program.
2. Open a new terminal window, then enter the following command:

   ```
   xhost + localhost
   ```

3. In the same window, become root by entering **su** and the root password.
4. Change to the root of the *GroupWise 6.5 for Linux Administrator* CD.
5. Enter **./install**.
6. Select the language in which you want to run the Installation Advisor and install the WebAccess software, then click Next.
7. In the Installation Advisor, click Install Products > GroupWise WebAccess > Install WebAccess Agent.
8. When the installation is complete, click OK.
9. Click Configure WebAccess Agent.
10. Follow the prompts to configure the Linux WebAccess Agent.
11. When installation and configuration is complete, you need to configure your GroupWise system so that the WebAccess and WebPublisher Applications know about this instance of the WebAccess Agent and can direct the appropriate user requests to it. For instructions, see "Configuring Redirection and Failover Support" on page 810.

Installing a Linux WebAccess and WebPublisher Application

To install a WebAccess Application and a WebPublisher Application to a Web server:

1. After installing and configuring the WebAccess Agent, click Install GroupWise WebAccess Application with Apache and Tomcat if you want to create a new installation of Apache and Tomcat for this instance of the WebAccess Application.

   or

   If you want to use an existing Apache and Tomcat installations, click Install GroupWise WebAccess Application.
2. When the installation is complete, click OK.
3. Click Configure WebAccess Application.
4. Follow the prompts to configure the Linux WebAccess Application.
5. When the installation and configuration is complete, start or restart the Web server.

Configuring Redirection and Failover Support

Redirection enables the WebAccess Application to direct user requests to specific WebAccess Agents. For example, you might want WebAccess Agent 1 to process all requests from users on Post Office 1 and WebAccess Agent 2 to process all requests from users on Post Office 2.

Failover support enables the WebAccess Application to contact a second WebAccess Agent if the first WebAccess Agent is unavailable. For example, if the WebAccess Application receives a user request that should be processed by WebAccess Agent 1 but it is unavailable, the WebAccess Application can route the user request to WebAccess Agent 2 instead.

The following sections provide information to help you successfully configure redirection and failover support:

- "How the WebAccess Application Knows Which WebAccess Agents to Use" on page 810
- "Synchronizing the Encryption Key" on page 812
- "Specifying a WebAccess Agent in the WebAccess URL" on page 813
- "Assigning a Default WebAccess Agent to a Post Office" on page 815
- "Assigning a Default WebAccess Agent to a Domain" on page 816
- "Adding WebAccess Agents to the GroupWise Service Provider's List" on page 817

How the WebAccess Application Knows Which WebAccess Agents to Use

To redirect user requests or to fail over to a second WebAccess Agent, the WebAccess Application needs to know which WebAccess Agents you want it to use. This might be all of the WebAccess Agents in your system, or only specific WebAccess Agents.

Each time a user logs in, the WebAccess Application compiles a list, referred to as a redirection/failover list, of the WebAccess Agents defined in the locations listed below.

- **The WebAccess URL.** The standard URL does not contain a WebAccess Agent, but you can modify the URL to point to a specific agent.
- **The user's Post Office object.** You can assign a default WebAccess Agent to the post office to handle requests from the post office's users.
- **The user's Domain object.** You can assign a default WebAccess Agent to the domain to handle requests from the domain's users.
- **The GroupWiseProvider object.** This is the service provider used by the WebAccess Application to connect to WebAccess Agents.
- **The commgr.cfg file.** This file located in the WebAccess Application's home directory (novell\webaccess on the Web server or /opt/novell/groupwise/webaccess on Linux).

By default, only the GroupWise Provider object and the commgr.cfg file include a WebAccess Agent definition, as shown in the following table:

Location	WebAccess Agent
WebAccess URL	No agent defined
Post office	No agent defined
Domain	No agent defined

Location	WebAccess Agent
GroupWise service provider	Agent 1
Commgr.cfg	Agent 1

If no other WebAccess Agents are defined (as is the case by default), the WebAccess Application will direct all user requests to the WebAccess Agent (Agent 1) listed in the commgr.cfg file. This file is located in the WebAccess Application’s home directory on the Web server. The commgr.cfg file contains the IP address and encryption key for the WebAccess Agent that was associated with the WebAccess Application during the application’s installation.

If Agent 1 is not available, the user will receive an error message and will be unable to log in.

Redirection/Failover List: Example 1

Assume that the WebAccess Agents are defined as follows:

Location	WebAccess Agent
WebAccess URL	No agent defined
Post office	Agent 1
Domain	Agent 4
GroupWise service provider	Agent 2 Agent 3
Commgr.cfg	Agent 4

Using this information, the WebAccess Application would create the following redirection/ failover list:

List Entry	Taken From
Agent 1	Post office
Agent 4	Domain
Agent 2	GroupWise service provider
Agent 3	GroupWise service provider

Because there is no WebAccess Agent defined in the WebAccess URL, the WebAccess Application will redirect the user’s request to the default WebAccess Agent (Agent 1) assigned to the user’s post office. If Agent 1 is unavailable, the WebAccess Application will fail over to the domain’s default WebAccess Agent (Agent 4). If Agent 4 is unavailable, the WebAccess Application will fail over to Agent 2 and then Agent 3, both of which are defined in the GroupWise service provider’s list.

Redirection/Failover List: Example 2

Assume that the WebAccess Agents are defined as follows:

Location	WebAccess Agent
WebAccess URL	No agent defined
Post office	No agent defined
Domain	No agent defined
GroupWise service provider	Agent 1 Agent 2 Agent 3
Commgr.cfg	Agent 2

Using this information, the WebAccess Application would create the following redirection/failover list:

List Entry	Taken From
Agent 1	GroupWise service provider
Agent 2	GroupWise service provider
Agent 3	GroupWise service provider

Because there is no WebAccess Agent defined in the WebAccess URL, user's post office, or user's domain, the WebAccess Application will redirect the user's request to the first WebAccess Agent (Agent 1) in the GroupWise service provider's list. If Agent 1 is unavailable, the WebAccess Application will fail over to Agent 2 and then Agent 3.

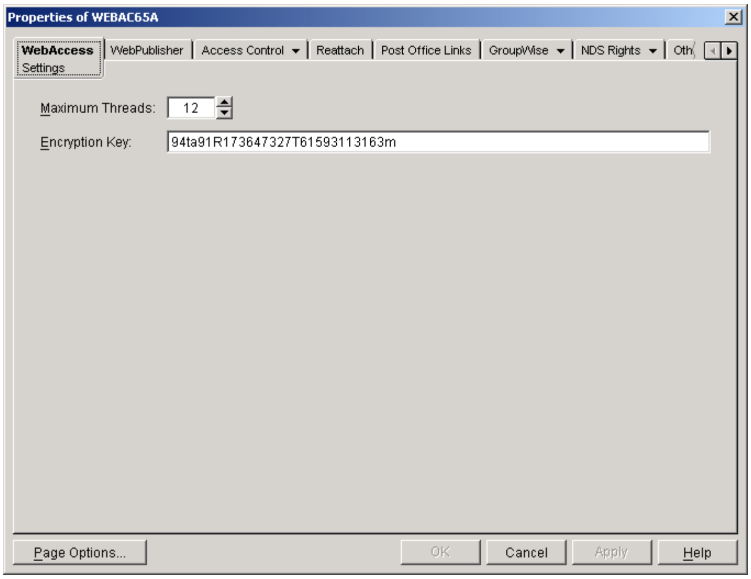
Synchronizing the Encryption Key

Every WebAccess Agent has an encryption key. In order to communicate with a WebAccess Agent, the WebAccess Application must know the agent's encryption key. The encryption key is randomly generated when the WebAccess Agent object is created in eDirectory, which means that every WebAccess Agent has a unique encryption key.

If a WebAccess Application will communicate with more than one WebAccess Agent, all the WebAccess Agents must use the same encryption key.

To modify a WebAccess Agents encryption key:

1. In ConsoleOne®, right-click the WebAccess Agent object, then click Properties.
2. If necessary, click the WebAccess tab to display the WebAccess Settings page.



Maximum Threads: 12

Encryption Key: 94ta91R173647327T61593113163m

3 Make the encryption key the same as the key for any other WebAccess Agents with which the WebAccess Application communicates.

4 Click OK to save the changes.

Specifying a WebAccess Agent in the WebAccess URL

To have the WebAccess Application connect to a WebAccess Agent other than the one specified in the commgr.cfg file, you can add the WebAccess Agent's IP address and port number to the URL that calls the WebAccess Application. For example, the default WebAccess Application URL is:

NetWare and Windows: http://*web_server_ip_address*/servlet/webacc
Linux: http://*web_server_ip_address*/gw/webacc

This URL causes the WebAccess Application to use the IP address and port number that is listed in the commgr.cfg file. To redirect the WebAccess Application to another WebAccess Agent, you would use the following URLs:

NetWare and Windows: http://*web_server_ip_address*/servlet/webacc
?GWAP.ip=*agent_ip_address*&GWAP.port=*port_number*
Linux: http://*web_server_ip_address*/gw/webacc
?GWAP.ip=*agent_ip_address*&GWAP.port=*port_number*

For example:

NetWare and Windows: http://151.155.123.45/servlet/webacc
?GWAP.ip=151.155.789.10&GWAP.port=7204
Linux: http://151.155.123.45/gw/webacc
?GWAP.ip=151.155.789.10&GWAP.port=7204

In this example, the WebAccess Application will redirect its requests to the WebAccess Agent at IP address 151.155.789.10 and port number 7204. If the WebAccess Agent is using the same port number that is listed in the commgr.cfg file, you do not need to include the GWAP.port parameter. Or, if the WebAccess Agent is using the same IP address that is listed in the commgr.cfg file, you do not need to include the GWAP.ip parameter.

If you want, you can use the WebAccess Agent's DNS hostname in the URL rather than its IP address.

You can also specify the user interface language by adding the &User.lang option. This allows you to bypass the initial WebAccess language page. For example:

NetWare and Windows: http://151.155.123.45/servlet/webpub
?GWAP.ip=151.155.789.10&GWAP.port=7204&User.lang=en
Linux: http://151.155.123.45/gw/webpub
?GWAP.ip=151.155.789.10&GWAP.port=7204&User.lang=en

You can use the language codes listed below with the &User.lang parameter in the WebAccess URL.

Language	Code	Language	Code
Arabic	ar	Hebrew	iw
Brazilian Portuguese	pt	Hungarian	hu
Chinese Simplified	cs	Italian	it
Chinese Traditional	ct	Japanese	jp
Czechoslovakian	cz	Korean	kr
Danish	da	Norwegian	no
Dutch	nl	Polish	pl
English	us	Russian	ru
Finnish	su	Spanish	es
French	fr	Swedish	sv
German	de		

You can add the URL to any Web page. For example, if you are using the Web Services page as your initial WebAccess page, you could add the URL to that page. You will need to add one URL for each WebAccess Agent.

For example, suppose you had offices in three different locations and installed a WebAccess Agent at each location to service the post offices at those locations. To enable the WebAccess Application to redirect requests to the WebAccess Agent at the appropriate location, you could modify the Web Services page to display a list of the locations. The modified page would include the following HTML code (if WebAccess is running on NetWare or Windows):

```
<UL>

<LI><A HREF="http://151.155.123.45/servlet/
webacc?GWAP.ip=151.155.789.10&GWAP.port=7204>San Francisco
</A></LI>

<LI><A HREF="http://151.155.123.45/servlet/
webacc?GWAP.ip=151.155.456.12>New York
</A></LI>

<LI><A HREF="http://151.155.123.45/servlet/
```

```
webacc?GWAP.ip=151.155.654.33&GWAP.port=7203>London
</A></LI>

</UL>
```

In the preceding example, in Linux, the directory “servlet” is replaced by “gw”.

The displayed HTML page would contain the following list of locations:

- San Francisco
- New York
- London

When a user selectes a location, the WebAccess Application will route all requests to the WebAccess Agent at the selected location.

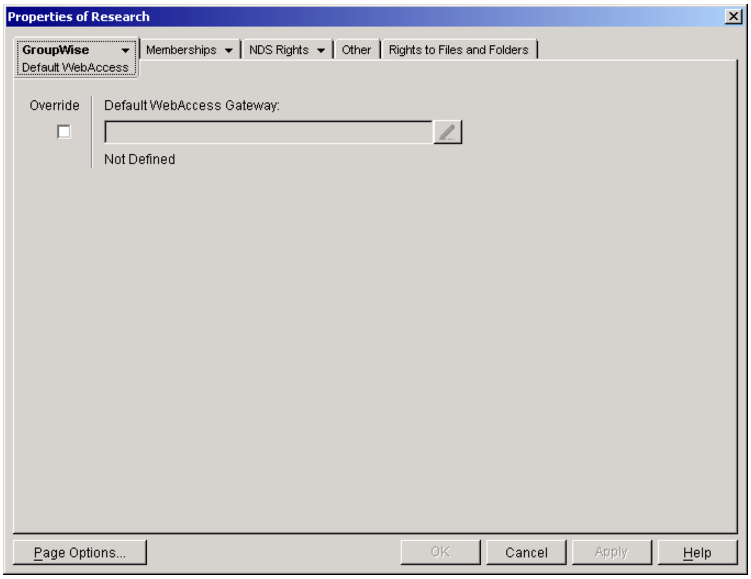
Assigning a Default WebAccess Agent to a Post Office

The WebAccess Application uses the post office’s default WebAccess Agent if no WebAccess Agent has been specified in the WebAccess URL (see “Specifying a WebAccess Agent in the WebAccess URL” on page 813) or if that WebAccess Agent is unavailable. This applies only if you have multiple WebAccess Agents installed in your GroupWise system. If you have only one WebAccess Agent, it services all post offices.

To assign a default WebAccess Agent to a post office:

1 In ConsoleOne, right-click the Post Office object, then click Properties.

2 Click GroupWise > Default WebAccess to display the Default WebAccess page.



Properties of Research

Override ☐

Default WebAccess Gateway:

Not Defined

3 Select the Override box to turn on the option.

4 In the Default WebAccess Gateway box, browse for and select the WebAccess Agent that you want to assign as the default agent.

When you have multiple WebAccess Agents and a user logs in to GroupWise WebAccess, the GroupWise Application running on the Web server checks to see if a default WebAccess Agent has been assigned to the user’s post office. If so, the WebAccess Application connects to the assigned WebAccess Agent. If not, it connects to the default WebAccess Agent assigned to the post office's domain, as described in "Assigning a Default WebAccess Agent to a Domain" on page 816 or to one of the WebAccess Agents in its service provider list, as described in "Adding WebAccess Agents to the GroupWise Service Provider's List" on page 817. If possible, select a WebAccess Agent that has good access to the post office to ensure the best performance.

5 Click OK to save the changes.

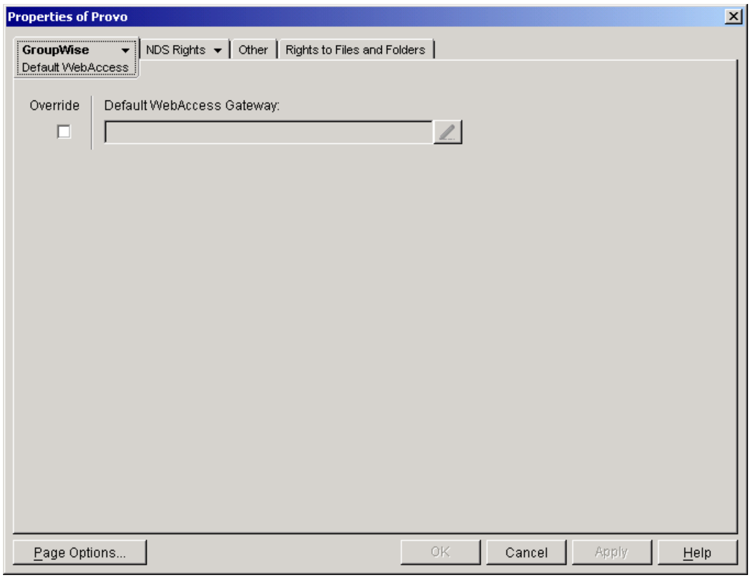
Assigning a Default WebAccess Agent to a Domain

The WebAccess Application uses the domain's default WebAccess Agent if 1) no WebAccess Agent has been specified in the WebAccess URL (see "Specifying a WebAccess Agent in the WebAccess URL" on page 813), 2) no default WebAccess Agent has been defined for the user's post office, or 3) neither of those WebAccess Agents are available. This applies only if you have multiple WebAccess Agents installed in your GroupWise system. If you have only one WebAccess Agent, it services users in all domains.

To assign a default WebAccess Agent to a domain:

1 In ConsoleOne, right-click the Domain object, then click Properties.

2 Click GroupWise > Default WebAccess to display the Default WebAccess page.



Override ☐

Default WebAccess Gateway:

3 Select the Override box to turn on the option.

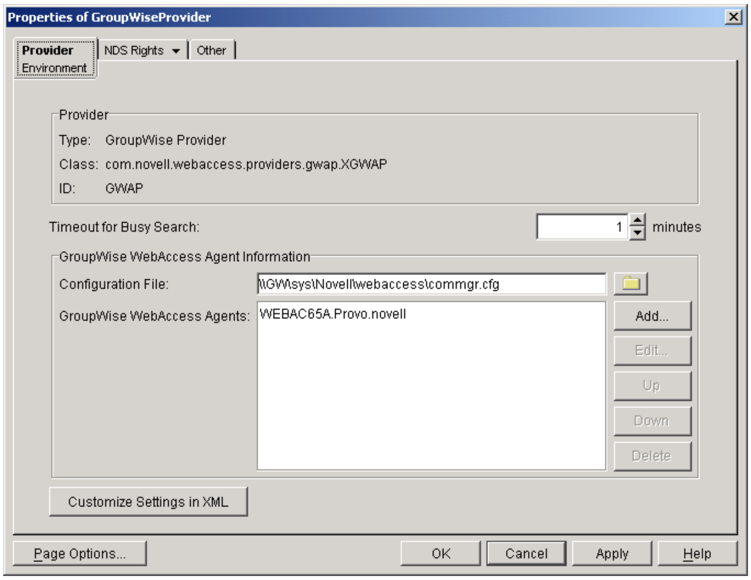
4 In the Default WebAccess Gateway box, browse for and select the WebAccess Agent that you want to assign as the default agent.

When you have multiple WebAccess Agents and a user logs in to GroupWise WebAccess, the GroupWise Application running on the Web server checks to see if a default WebAccess Agent has been assigned to the user's post office, as described in "Assigning a Default WebAccess Agent to a Post Office" on page 815. If so, the WebAccess Application connects to the assigned WebAccess Agent. If not, it connects to the default WebAccess Agent assigned to the post office's domain or to one of the WebAccess Agents in its service provider list, as described in "Adding WebAccess Agents to the GroupWise Service Provider's List" on page 817. If possible, you should select a WebAccess Agent that has good access to the domain's post offices to ensure the best performance. Each post office uses the domain's default WebAccess Agent unless you override the default at the post office level.

5. Click OK to save the changes.

Adding WebAccess Agents to the GroupWise Service Provider's List

1. In ConsoleOne, right-click the GroupWise service provider object (GroupWiseProvider), then click Properties.
2. If necessary, click the Provider tab to display the Environment page.



Provider

Type: GroupWise Provider

Class: com.novell.webaccess.providers.gwap.XGWAP

ID: GWAP

Timeout for Busy Search: 1 minutes

GroupWise WebAccess Agent Information

Configuration File: \\GW\sys\Novell\webaccess\commgr.cfg

GroupWise WebAccess Agents: WEBAC65A.Provo.novell

The GroupWise WebAccess Agents list displays the WebAccess Agents the GroupWise service provider can communicate with when attempting to complete a request. By default, the list includes the WebAccess Agent that is defined in the commgr.cfg file (listed in the Configuration File field). If the first WebAccess Agent is unavailable, the GroupWise service provider will attempt to use the second, third, fourth, and so on until it is successful.

3. Click Add, select the WebAccess Agent you want to add to the list, then click OK.
4. Repeat Step 3 for each WebAccess Agent you want to add to the list, then click OK to save the changes.

58 Controlling User Access

To control users' access to their mailboxes through GroupWise® WebAccess, you can do the following:

- Prevent users from logging in to their mailboxes through GroupWise WebAccess. By default, all GroupWise users can use WebAccess. See "Controlling User Access to Mailboxes" on page 819.
- Determine how long WebAccess users can remain inactive (no requests) before they are automatically logged out. The default is 20 minutes. See "Setting the Timeout Interval for Inactive Sessions" on page 825.
- Determine which WebAccess features (spell checking, LDAP directory searches, password modification, an so forth) are available to users. When WebAccess runs on NetWare or Windows, all features are available by default. When WebAccess runs on Linux, all features except opening attachments and LDAP directory searches are available by default. See "Configuring User Access to WebAccess Features" on page 826.

Controlling User Access to Mailboxes

You control which users have access to their mailboxes by creating classes of service and assigning users membership in a class. For example, if you don't want users on a particular post office to have access to their mailboxes through WebAccess, you can create a class of service that prevents access and then assign the entire post office membership in that class.

The following sections provide information to help you create and manage classes of service:

- "Class Membership" on page 819
- "Creating a Class of Service" on page 820
- "Adding Users to a Class of Service" on page 822
- "Maintaining the Access Database" on page 823

Class Membership

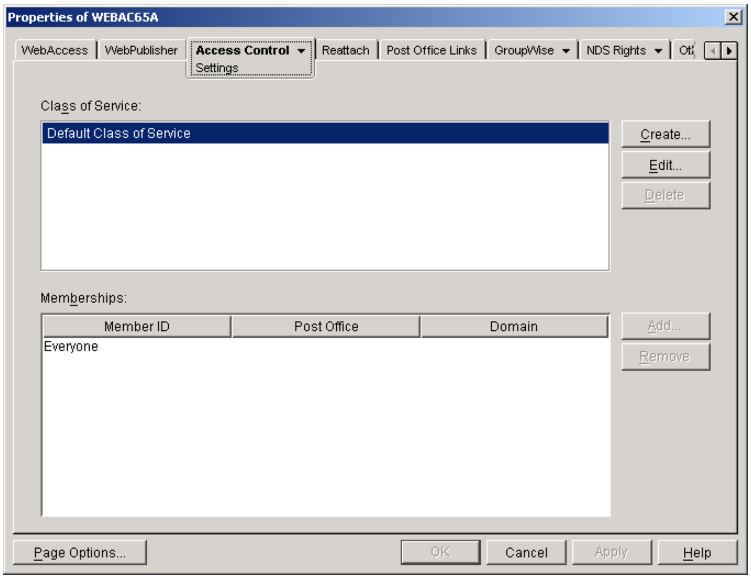
When you create a class of service, you assign membership in the class at a domain level, post office level, distribution list (group) level, or individual user level, which means that a user could be assigned membership in multiple classes. For example, a user might be a member in one class because his or her domain is a member; at the same time, the user is a member in another class because his or her post office is a member of that class. Because each user can have only one class of service, membership conflicts are resolved hierarchically, as shown below:

Membership assigned to a user through a...	Overrides membership assigned to the user through the...
domain	◆ default class of service
post office	◆ default class of service ◆ domain
distribution list	◆ default class of service ◆ domain ◆ post office
user	◆ default class of service ◆ domain ◆ post office

If a user's membership in two classes of service is based upon the same level of membership (for example, both through individual user membership), the class that applies is the one that allows the most privileges. For example, if the user belongs to one class of service that allows access to WebAccess and another class that prevents access, the class that allows access applies to the user.

Creating a Class of Service

1. In ConsoleOne®, right-click the WebAccess Agent object, then click Properties.
2. Click Access Control > Settings to display the Access Control Settings page.



Properties of WEBAC65A

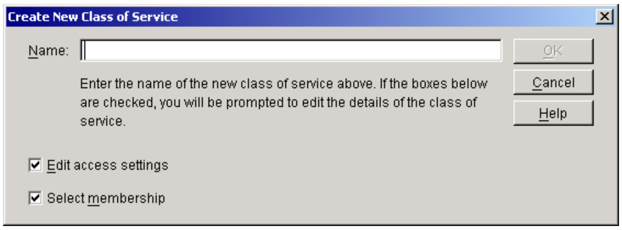
Class of Service:

Default Class of Service

Memberships:

Member ID	Post Office	Domain
Everyone		

3. Click Create to display the Create New Class of Service dialog box.


Create New Class of Service

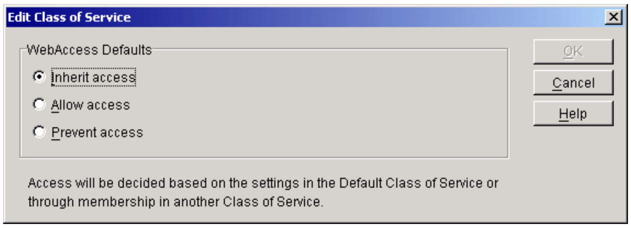
Name:

Enter the name of the new class of service above. If the boxes below are checked, you will be prompted to edit the details of the class of service.

☑ Edit access settings

☑ Select membership

4 Type a name for the class, then click OK to display the Edit Class of Service dialog box.


Edit Class of Service

WebAccess Defaults

● Inherit access

○ Allow access

○ Prevent access

Access will be decided based on the settings in the Default Class of Service or through membership in another Class of Service.

5 Select one of the following options:

Inherit Access: Select this option if you want members of this class of service to inherit their access from the default class of service or another class of service that they have membership in.

Allow Access: Select this option to enable members of the class to use WebAccess.

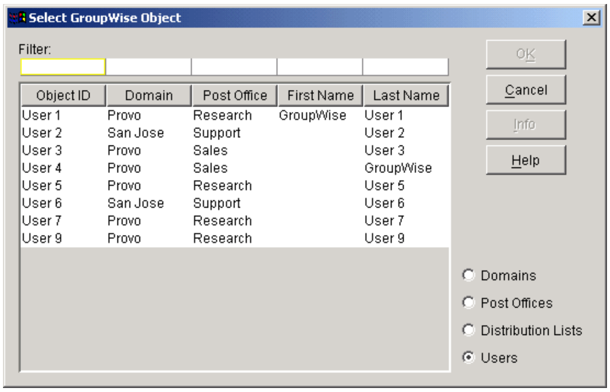
If you select Allow Access, you must also set a timeout interval. The timeout interval determines how long the WebAccess Agent keeps open a dedicated connection to the post office on behalf of the user. If the agent does not receive a user request within the specified interval, it closes the user's connection to the post office in order to free up its resources and the Post Office Agent's resources for other uses.

When the WebAccess Agent closes a user's connection to the post office, the user is not logged out of WebAccess. The user can continue to use WebAccess. As soon as the agent receives a request from the user, it opens the user's connection again. In general, you will want to leave the timeout interval set to the default 20 minutes.

You can also have users automatically logged out of WebAccess after a specified period of activity. WebAccess logout is handled by the WebAccess Application running on the Web server, not by the WebAccess Agent. For information, see "Setting the Timeout Interval for Inactive Sessions" on page 825.

Prevent Access: Select this option to prevent members of the class from using WebAccess.

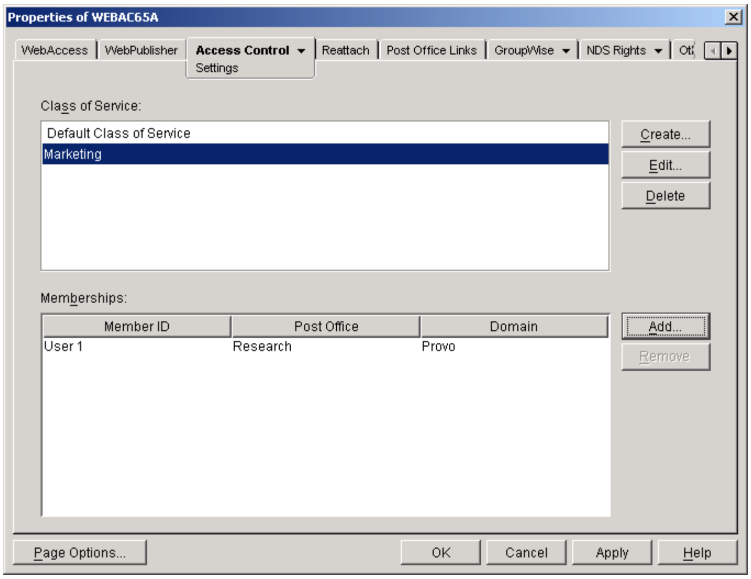
6 Click OK to display the Select GroupWise Object dialog box.



Object ID	Domain	Post Office	First Name	Last Name
User 1	Provo	Research	GroupWise	User 1
User 2	San Jose	Support		User 2
User 3	Provo	Sales		User 3
User 4	Provo	Sales		GroupWise
User 5	Provo	Research		User 5
User 6	San Jose	Support		User 6
User 7	Provo	Research		User 7
User 9	Provo	Research		User 9

7 Click Domains, Post Offices, Distribution Lists, or Users to display the list you want.

8 In the list, select the domain, post office, distribution list, or user you want, then click Add to add the object as a member in the class. You can Control-click or Shift-click to select multiple users.



Class of Service:

Default Class of Service
Marketing

Memberships:

Member ID	Post Office	Domain
User 1	Research	Provo

9 To add additional domains, post offices, distribution lists or users as members of the class of service, select the class of server, then click Add to display the Select GroupWise Object dialog box.

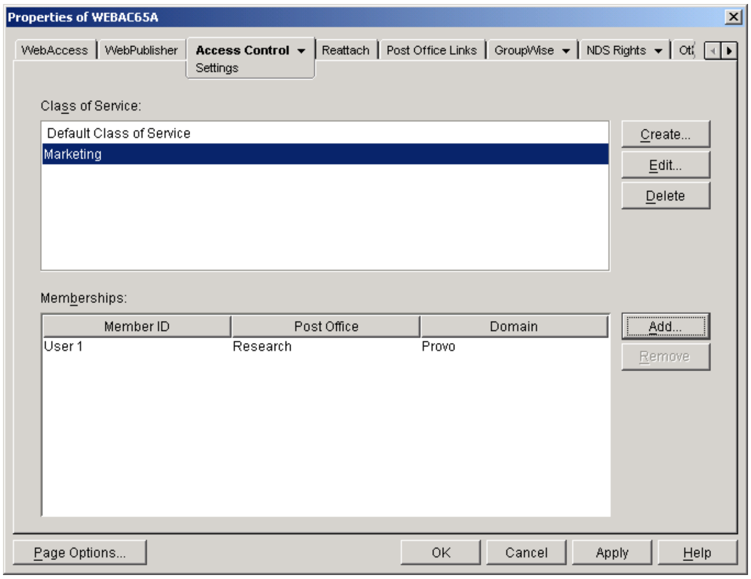
10 Click OK (on the Settings page) when finished adding members.

Adding Users to a Class of Service

The following steps help you add users to an existing class of service. For information about adding new classes of service, see "Creating a Class of Service" on page 820.

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

2 Click Access Control > Settings to display the Access Control Settings page.



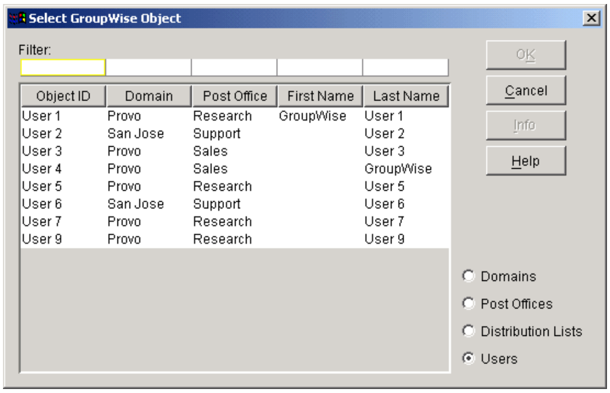
Class of Service:

- Default Class of Service
- Marketing

Memberships:

Member ID	Post Office	Domain
User 1	Research	Provo

3 In the Class of Service list, select the class you want to add members to, then click Add to display the Select GroupWise Object dialog box.



Object ID	Domain	Post Office	First Name	Last Name
User 1	Provo	Research	GroupWise	User 1
User 2	San Jose	Support		User 2
User 3	Provo	Sales		User 3
User 4	Provo	Sales		GroupWise
User 5	Provo	Research		User 5
User 6	San Jose	Support		User 6
User 7	Provo	Research		User 7
User 9	Provo	Research		User 9

○ Domains
○ Post Offices
○ Distribution Lists
● Users

4 Click Domains, Post Offices, Distribution Lists, or Users to display the list you want.

5 In the list, select the domain, post office, distribution list, or user you want, then click Add to add the object as a member in the class.

6 Repeat Step 3 through Step 5 for each object you want to add.

Maintaining the Access Database

The Access database stores the information for the classes of service you have set up to control user access to GroupWise WebAccess. When problems occur, you can validate the database to check for physical inconsistencies with the database's records and indexes. If inconsistencies are found, you can recover the database.

The Access database, gwac.db, is located in the *domain*\wpgate*webac65a* directory.

This section includes the following information:

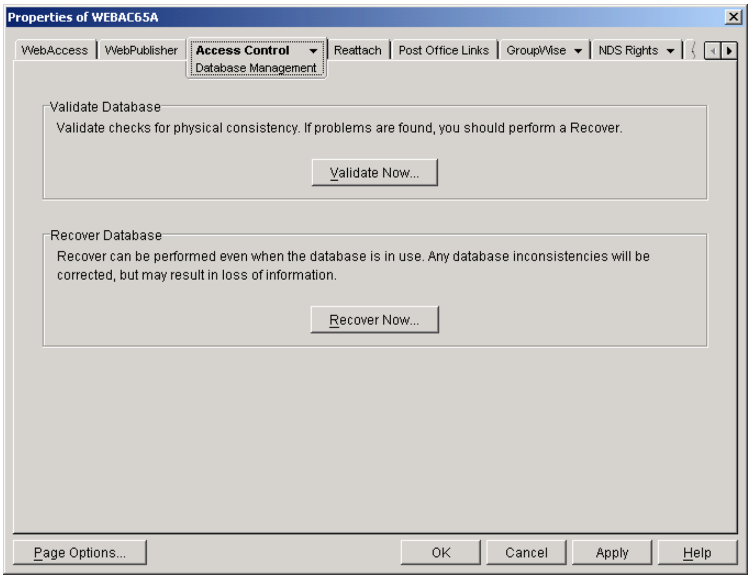
- "Validating the Access Database" on page 824
- "Recovering the Access Database" on page 824

Validating the Access Database

Validating the Access database checks for physical inconsistencies with the database's records and indexes.

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

2 Click Access Control > Database Management to display the Database Management page.



Validate checks for physical consistency. If problems are found, you should perform a Recover.

Recover can be performed even when the database is in use. Any database inconsistencies will be corrected, but may result in loss of information.

3 Click Validate Now.

4 After the database has been validated, click OK.

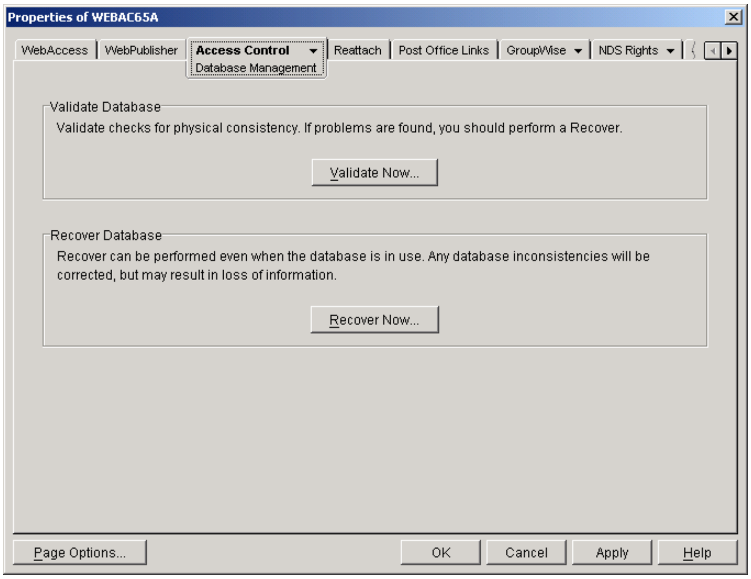
If inconsistencies were found, see "Recovering the Access Database" on page 824.

Recovering the Access Database

When you recover the Access database, a new database is created and all salvageable records are copied to the new database. Because some records might not be salvageable, after the recovery you will want to check the classes of services you have defined to see if any information was lost.

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

2 Click Access Control > Database Management to display the Database Management page.



Validate checks for physical consistency. If problems are found, you should perform a Recover.

Recover can be performed even when the database is in use. Any database inconsistencies will be corrected, but may result in loss of information.

3 Click Recover Now.

4 After the database has been recovered, click OK.

Setting the Timeout Interval for Inactive Sessions

By default, users will be logged out of GroupWise WebAccess after 20 minutes if they have not performed any actions that generate requests. Actions such as opening or sending a message generate requests. Other actions, such as scrolling through the Item List, composing a mail message without sending it, and reading Help topics, do not generate requests.

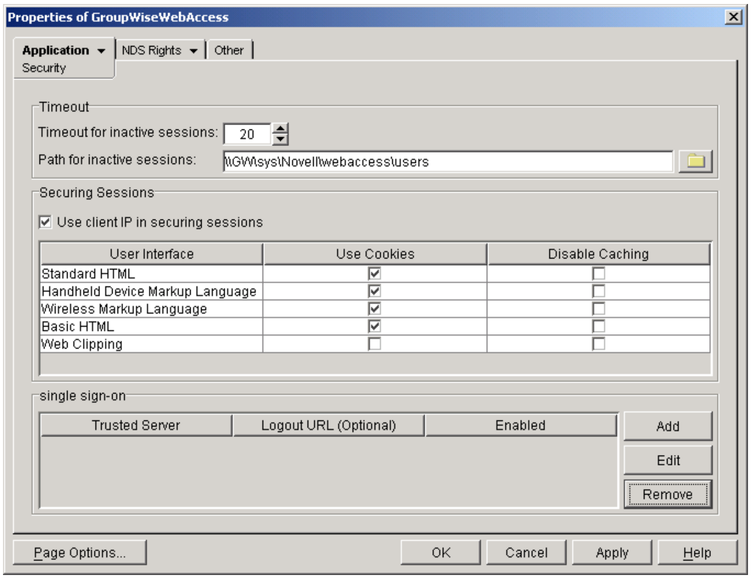
The timeout interval provides security for WebAccess users who forget to log out. It also helps the performance of the Web server by freeing the resources dedicated to that user's connection.

The WebAccess Application on the Web server controls the timeout. At the time the user is logged out, the WebAccess Application saves the user's current session to a directory on the Web server, where it is stored for 24 hours. If the logged-out user attempts to continue the session, he or she will be prompted to log in again, after which the WebAccess Application will renew the session. For example, suppose a user is composing a message when the timeout interval expires and then attempts to send the message. The user will be prompted to log in again, after which the message will be sent. No information is lost.

IMPORTANT: This timeout interval is different than the one you can establish when creating a class of service (see "Creating a Class of Service" on page 820). That timeout interval determines how long the WebAccess Agent will keep open a session with an inactive user, and this timeout interval determines how long the WebAccess Application will maintain an inactive session. In general, if the WebAccess Agent session times out, users will not notice; the next time they make a request, the WebAccess Agent will open a new session. However, if the WebAccess Application session times out, users will be prompted to log in again.

To modify the timeout interval:

1 In ConsoleOne, right-click the WebAccess Application object, click Properties, then click Application > Security to display the Security page.



Timeout

Timeout for inactive sessions: 20

Path for inactive sessions: \\GW\sys\Novell\webaccess\users

Securing Sessions

☑ Use client IP in securing sessions

User Interface	Use Cookies	Disable Caching
Standard HTML	☑	□
Handheld Device Markup Language	☑	□
Wireless Markup Language	☑	□
Basic HTML	☑	□
Web Clipping	□	□

single sign-on

Trusted Server	Logout URL (Optional)	Enabled

2 In the Timeout for Inactive Sessions box, select the number of minutes for the timeout interval.

3 In the Path for Inactive Sessions box, select the path for the directory where you want inactive sessions stored.

4 Click OK.

The timeout interval applies to all users who log in through the Web server where the WebAccess Application is running. You cannot set individual user timeout intervals. However, if you have multiple Web servers, you can set different timeout intervals for the Web servers by completing the above steps for each server's WebAccess Application.

Configuring User Access to WebAccess Features

By default, WebAccess users can:

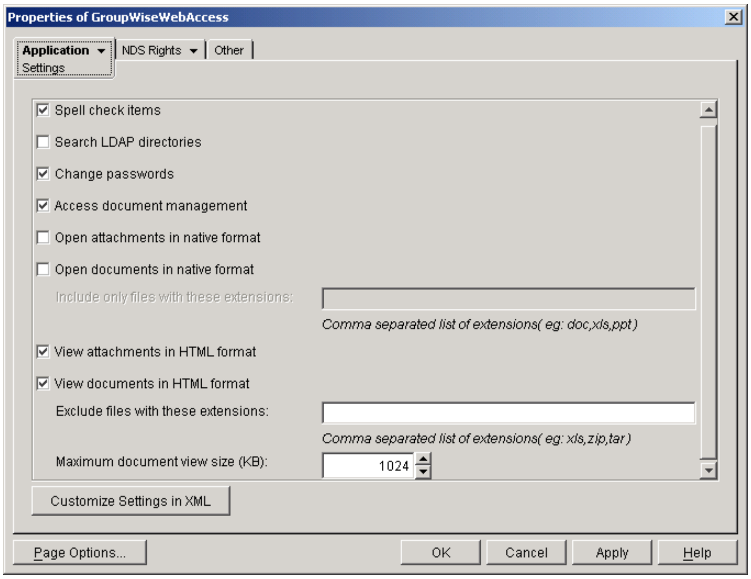
- Spell check messages
- Search LDAP directories (must be manually enabled on Linux)
- Change their GroupWise mailbox passwords
- Use Document Management Services
- Open attachments in native format (must be manually enabled on Linux)
- Open documents in native format (must be manually enabled on Linux)
- View attachments in HTML format
- View documents in HTML format

Access to these features is controlled by the WebAccess Application on the Web server. All users who log in through the Web server will have the same feature access. You cannot configure individual user settings. However, if you have multiple Web servers, you can establish different settings for the Web servers by completing the following steps for each server's WebAccess Application.

To configure the WebAccess feature settings:

1 In ConsoleOne, right-click the WebAccess Application object, then click Properties.

2 Click Application > Settings to display the Application Settings page.



☑ Spell check items

□ Search LDAP directories

☑ Change passwords

☑ Access document management

□ Open attachments in native format

□ Open documents in native format

Include only files with these extensions:

Comma separated list of extensions(eg: doc,xls,ppt)

☑ View attachments in HTML format

☑ View documents in HTML format

Exclude files with these extensions:

Comma separated list of extensions(eg: xls,zip,tar)

Maximum document view size (KB): 1024

3 Configure the following settings:

Spell Check Items: Enable this option if you want users to be able to use the Novell® Speller to spell check an item's text before sending the item. Disable this option to remove all Spell Check features from the user interface.

Search LDAP Directories: Enable this option if you have an LDAP server and you want users to be able to search any LDAP address books you have defined. Disable this option to remove all LDAP features from the user interface.

Change Passwords: Enable this option if you want users to be able to change their Mailbox passwords. Disable this option to remove all Password features from the user interface.

Access Document Management: Enable this option if you want users to be able to use the Document Management features. Disable this option to remove all Document Management features from the user interface.

Open Attachments in Native Format: By default, the Save As option enables users to save message attachments to their local drives and then open them in their native applications. You can turn on this option to enable the Open option. The Open option enables users to open message attachments directly in their native applications without first saving the files to the local drive.

This option requires that 1) each user's Web browser knows the correct application or plug-in to associate with the attachment, according to its file extension or MIME type, and 2) the application or plug-in is available to the user. Otherwise, the user will be prompted to save the file to disk or specify the application to open it.

This option and the View Attachments in HTML Format option can both be enabled at the same time. Doing so gives users both the Open option and the View option, which means they have the choice of opening an attachment in its native application or viewing it as HTML.

Open Documents in Native Format: By default, the Save As option enables user to save library documents to their local drives and then open them in their native applications. You can turn on this option to enable the Open option. The Open option enables users to open documents directly in their native applications without first saving the files to the local drive.

This option requires that 1) each user's Web browser knows the correct application or plug-in to associate with the document, according to its file extension or MIME type, and 2) the application or plug-in is available to the user. Otherwise, the user will be prompted to save the file to disk or specify the application to open it.

This option and the View Documents in Native Format option can both be enabled at the same time. Doing so gives users both the Open option and the View option, which means they have the choice of opening a document in its native application or viewing it as HTML.

If you want only certain file types to be have the Open option, enter the file types in the Include Only Files With These Extensions field. Include only the extension and separate each extension with a comma (for example, doc, xls, ppt). The Open option will not be available for any file types not entered in this field.

View Attachments in HTML Format: Enable this option if you want users to be able to view any type of attachments in HTML format. Disable this option to require users to save an attachment to a local drive and view it in its native application. WebAccess uses Stellent* Outside In* HTML Export to convert files to HTML format.

For a list of the supported file format conversions, download the following document from the Stellent Web site:

OutSide In Supported Platforms and File Formats (http://www.stellent.com/stellent3/groups/mkt/documents/nativepage/outside_in_supported_platforms.pdf)

This option and the Open Attachments in Native Format option can both be enabled at the same time. Doing so gives users both the View option and the Open option, which means they have the choice of viewing an attachment as HTML or opening it in its native application.

View Documents in HTML Format: Enable this option if you want users to be able to view library documents in HTML format. Disable this option to require users to save a document to a local drive and view it in its native application. WebAccess uses Stellent Outside In HTML Export to convert files to HTML format.

For a list of the supported file format conversions, download the following document from the Stellent Web site:

OutSide In Supported Platforms and File Formats (http://www.stellent.com/stellent3/groups/mkt/documents/nativepage/outside_in_supported_platforms.pdf)

This option and the Open Documents in Native Format option can both be enabled at the same time. Doing so gives users both the View option and the Open option, which means they have the choice of viewing a document as HTML or opening it in its native application.

If you want to exclude certain file types from having the View option, enter the file types in the Exclude Files With These Extensions field. Include only the extension and separate each extension with a comma (for example, doc, xls, ppt). The View option will be available for any file types not entered in this field.

4 Click OK.

59 Configuring WebAccess Components

WebAccess consists of a number of components that can be configured to meet the specific needs of your GroupWise system:

- "Configuring the WebAccess Agent" on page 829
- "Configuring the WebAccess Application" on page 841
- "Configuring the Novell Speller Application" on page 854
- "Configuring the WebPublisher Application" on page 857
- "Configuring the GroupWise Service Provider" on page 867
- "Configuring the LDAP Service Provider" on page 868
- "Configuring the GroupWise Document Service Provider" on page 869

Configuring the WebAccess Agent

During installation, the GroupWise® WebAccess Agent is set up with a default configuration. On Linux, this happens during the configuration step. However, you can use the information in the following sections to optimize the WebAccess Agent for your environment:

- "Modifying WebAccess Settings" on page 829
- "Modifying WebPublisher Settings" on page 830
- "Controlling WebAccess Agent Logging" on page 832
- "Managing Access to Post Offices" on page 837
- "Changing the WebAccess Agent's Network Address or Port Numbers" on page 840

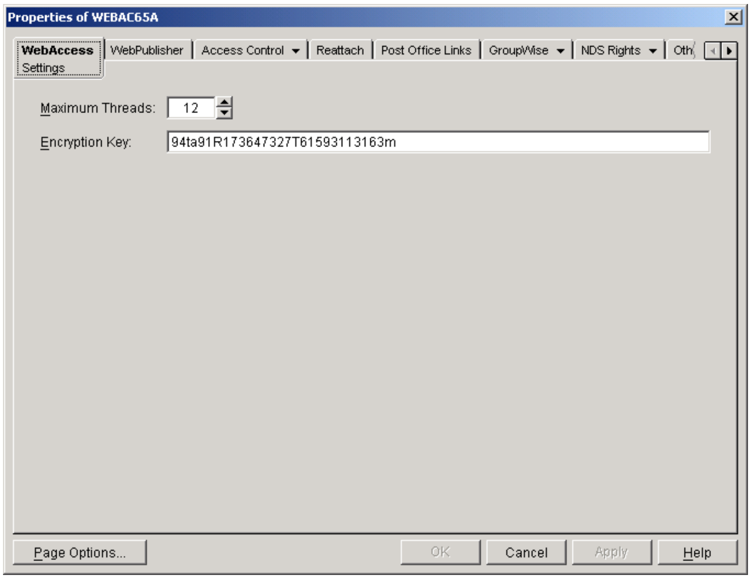
Modifying WebAccess Settings

Using ConsoleOne®, you can configure the following GroupWise WebAccess settings for the WebAccess Agent:

- The maximum number of threads the agent will use to process WebAccess messages
- The key used to encrypt information sent between the agent and the WebAccess Application

To modify the configuration information:

1. In ConsoleOne, right-click the WebAccess Agent object, then click Properties.
2. If necessary, click WebAccess > Settings to display the WebAccess Settings page.



Maximum Threads: 12

Encryption Key: 94ta91R173647327T61593113163m

3 Modify any of the following fields:

Maximum Threads: This is the maximum number of threads the agent will use at one time to process requests. The default (12) enables the agent to process 12 requests at one time, which is usually sufficient. If the agent regularly receives more requests than it has threads, you might want to increase the maximum number of threads. Increasing the threads increases the amount of server memory used by the agent.

To determine the maximum number of threads that have been in use at one time (for example, 8 of the 12 threads), you can view the server console screen for the NetWare® WebAccess Agent or view the status information displayed through the Web console. See "Monitoring the WebAccess Agent" on page 875.

Encryption Key: The encryption key is used to encrypt and decrypt the information sent between the WebAccess Agent and the WebAccess Application. If you do not want to use the default encryption key, you can type your own key. The encryption key must be identical to the encryption keys of any other WebAccess Agents that the WebAccess Application communicates with. For more information, see "Configuring Redirection and Failover Support" on page 810.

4 Click OK to save the changes.

Modifying WebPublisher Settings

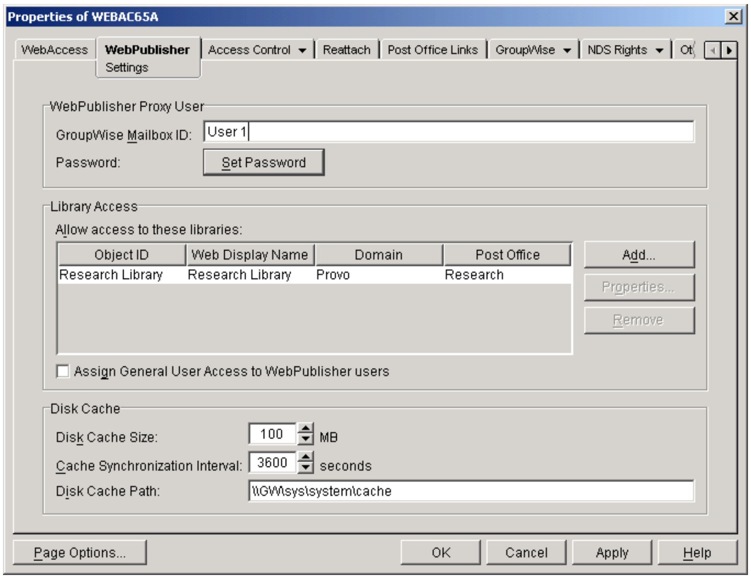
Using ConsoleOne, you can configure the following WebPublisher settings for the WebAccess Agent:

- The GroupWise account used by the WebAccess Agent to retrieve documents for WebPublisher users
- The GroupWise libraries where the WebAccess Agent will look for documents that have been shared with GroupWise WebPublisher users
- The maximum amount of disk space to use when caching documents that have been converted to HTML for viewing by GroupWise WebPublisher users
- How often to synchronize the cached documents with the original documents in the GroupWise libraries
- The location where the files will be cached

To modify the configuration information:

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

2 Click WebPublisher > Settings to display the WebPublisher Settings page.



WebPublisher Proxy User

GroupWise Mailbox ID: User 1

Password:

Library Access

Allow access to these libraries:

Object ID	Web Display Name	Domain	Post Office
Research Library	Research Library	Provo	Research

□ Assign General User Access to WebPublisher users

Disk Cache

Disk Cache Size: 100 MB

Cache Synchronization Interval: 3600 seconds

Disk Cache Path: \\GW\sys\system\cache

3 Modify any of the following fields:

GroupWise Mailbox ID: The WebPublisher proxy user serves two purposes: 1) GroupWise users make documents available to GroupWise WebPublisher users by sharing the documents with the WebPublisher proxy user and 2) the WebAccess Agent logs in to GroupWise through the WebPublisher proxy user. This enables the WebAccess Agent to search for and retrieve documents that have been shared with the WebPublisher proxy user. Specify the ID for the GroupWise mailbox you want to use.

Password: Click Set Password to specify the mailbox password.

Allow Access to These Libraries: This list displays the libraries that the WebAccess Agent has access to. If a library is not in the list, WebPublisher users cannot see the library's documents. If a library is listed, WebPublisher users can view any of the library's documents that have been shared (by the document owner) with the WebPublisher proxy user.

To add a library to the list, click Add, then browse for and select the library.

To change the display name or description for the library, select the library, then click Properties. By default, the library's Novell® eDirectory™ object name is used for the display name.

To remove a library from the list, select the library, then click Remove.

Assign General User Access to WebPublisher Users: When sharing documents with GroupWise users, a document's owner can assign individual access rights and general access rights (through the General User Access option). The General User Access rights determine the access for all GroupWise users who do not receive individual access rights. For example, if a document's owner sets the General User Access to View, all GroupWise users with access to that library can view the document.

This option lets you determine whether or not you, as the GroupWise system administrator, want to give General User Access rights to WebPublisher users. For example, with this option enabled, WebPublisher users can view any documents that have General User Access set to View.

Disk Cache Size: When a GroupWise WebPublisher user requests a document from a GroupWise library, the WebAccess Agent retrieves the document, renders it to HTML, displays it to the GroupWise WebPublisher user, and then saves it to a disk cache. If the document is requested again, the cached version is used.

The disk cache size determines the maximum amount of disk space to be used for the cache. The default is 100 MB. If there is not room in the cache for a newly rendered document, the least recently requested document is removed from the cache to make room for the new document.

If GroupWise users are publishing large numbers of documents, you might want to increase the cache size. The advantage of a large cache is that cached documents are displayed more quickly to GroupWise WebPublisher users because the WebAccess Agent does not have to first render them to HTML. The disadvantage of a large cache is the disk space used and the amount of time required by the WebAccess Agent to keep the cached documents synchronized with the original documents.

Cache Synchronization Interval: The cache synchronization interval determines how often the WebAccess Agent checks for differences between the cached documents and the original documents in the library. Based on the default interval, the WebAccess Agent checks for differences every one hour (3600 seconds). If differences exist, the WebAccess Agent replaces the cached document with a newly rendered version of the original document.

Disk Cache Path: The disk cache path indicates the directory where documents are stored. By default, this is a directory on the WebAccess Agent's server (c:\groupwise\cache for Windows or sys:\system\cache for NetWare® or /opt/novell/groupwise/webpublisher/cache for Linux). If necessary, you can change the path to specify a new location.

To increase speed and reduce network traffic, we recommend that you keep the cache directory on the WebAccess Agent's server.

4 Click OK to save the changes.

Controlling WebAccess Agent Logging

The WebAccess Agent provides logging options to help you monitor the operation of the agent.

The following sections explain the how to control logging:

- "Controlling the Agent's Logging" on page 832
- "Assigning Operators to Receive Warning and Error Messages" on page 836

Controlling the Agent's Logging

The WebAccess Agent logs information to the console and to a log file on disk (by default, disk logging is turned off). You can control the following logging features:

- The type of information to log.
- Whether disk logging is on or off.
- How long to retain log files.
- The maximum amount of disk space to use for log files.
- Where to store log files.

You can control logging through ConsoleOne, WebAccess Agent startup switches, and the WebAccess Agent console. The following table shows which logging options you can control from each location.

	ConsoleOne	Startup Switches	NetWare Console	NetWare Console	Linux Console
Logging Level	Yes	Yes	Yes	Yes	No
Disk Logging	Yes	Yes	Yes	No	No
Maximum Log File Age	Yes	Yes	Yes	No	No
Maximum Disk Space	Yes	Yes	Yes	No	No
Log File Location	Yes	Yes	No	Yes	No

The log settings in ConsoleOne are used as the default settings. Startup switches override the ConsoleOne log settings, and agent console settings override startup switches and ConsoleOne settings for the current agent session. For information about modifying log settings through ConsoleOne, startup switches, or the WebAccess Agent console, see the following sections:

- "Modifying Log Settings in ConsoleOne" on page 833
- "Modifying Log Settings through Startup Switches" on page 834
- "Modifying Log Settings through the NetWare Agent's Console" on page 835
- "Modifying Log Settings through the Windows Agent's Console" on page 836
- "Modifying Log Settings on Linux" on page 836

Modifying Log Settings in ConsoleOne

Through ConsoleOne, you can select the following log settings:

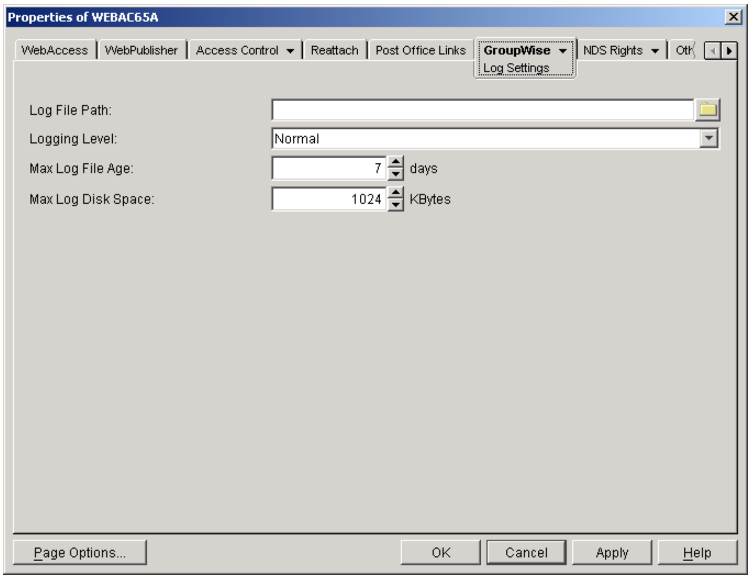
- Log file location
- Logging level
- Maximum age for log files
- Maximum disk spaced used for log files

By default, the WebAccess Agent does not log information to a file on disk on NetWare and Windows. (However, on Linux, it does.) To turn disk logging on, you can use the /logdiskon startup switch. See "Modifying Log Settings through Startup Switches" on page 834. If you are using the NetWare WebAccess Agent, you can turn disk logging on through the agent's console. See "Modifying Log Settings through the NetWare Agent's Console" on page 835.

The WebAccess Agent creates a new log file each day and each time it is started. The log file is named *mmdd*web.*nnn*, where *mm* is the month, *dd* is the day, and *nnn* is a sequenced number (001 for the first log file of the day, 002 for the second, and so forth). On NetWare and Windows, the default location for the log files is the *domain*\wpgate*webac65a*\000.prc directory. On Linux, the location is /var/log/novell/groupwise/*domain_name.gateway_name*/000.prc.

To modify log settings in ConsoleOne:

1. In ConsoleOne, right-click the WebAccess Agent object, then click Properties.
2. Click GroupWise > Log Settings to display the Log Settings page.



Log File Path:

Logging Level: Normal

Max Log File Age: 7 days

Max Log Disk Space: 1024 KBytes

3 Modify any of the following properties:

Log File Path: By default, this field is empty. If you have turned on disk logging by using the /logdiskon startup switch (see "Modifying Log Settings through Startup Switches" on page 834), the log files will be saved to the default directory or to the directory specified by the /log startup switch. If you want to specify a different location, enter the directory path or browse to and select the directory.

If you have not used the /logdiskon startup switch to turn on logging, entering a log file path will activate disk logging (after you restart the WebAccess Agent).

Logging Level: There are four logging levels: Off, Normal, Verbose, and Diagnostic. Off turns logging off; Normal displays initial statistics, user logins, warnings, and errors; Verbose displays normal logging plus user requests; and Diagnostic displays Verbose logging plus thread information. The default is Normal logging. Use Diagnostic only if you are troubleshooting a problem with WebAccess.

The verbose and diagnostic logging levels do not degrade WebAccess Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Max Log File Age: Specify the number of days you want the WebAccess Agent to retain old log files. The WebAccess Agent will retain the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.

Max Log Disk Space: Specify the maximum amount of disk space you want to use for log files. If the disk space limit is exceeded, the WebAccess Agent will delete log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 1024 KB.

4 Click OK to save the log settings.

Modifying Log Settings through Startup Switches

Startup switches override any log settings you specified through ConsoleOne. See "Modifying Log Settings in ConsoleOne" on page 833.

To use a switch, you can:

- Add the switch to the command line. For example, load gwinter.nlm /ph-j:\domain\wpgate\webac65a.

- On NetWare, include the switch in the WebAccess NetWare configuration file (strtweb.ncf), typically located in sys:\system.
- On Linux, include the switch in the WebAccess startup script (*gateway_name*.waa) located in /opt/novell/groupwise/agents/bin.
- On Windows, include the switch in the WebAccess startup batch file (strtweb.bat), typically located in c:\webacc.

For information about startup switches that can be used to modify log settings, see "Using WebAccess Agent Startup Switches" on page 895.

Modifying Log Settings through the NetWare Agent's Console

You can use the NetWare WebAccess Agent's console to modify the following log settings:

- Logging level
- Disk logging on or off
- Maximum age for log files
- Maximum disk space used for log files

Changes you make to log settings at the console apply only to the current session. When you restart the WebAccess Agent, the log settings are reset to the settings specified in ConsoleOne or the startup switches. See "Modifying Log Settings in ConsoleOne" on page 833 and "Modifying Log Settings through Startup Switches" on page 834.

To modify the log settings:

1. At the NetWare WebAccess Agent's console, press F10, select Logging Options, then modify any of the following settings:

   Logging Level: Off turns logging off; Normal displays initial statistics, user logins, warnings, and errors; Verbose displays normal logging plus user requests; and Diagnostic displays Verbose logging plus thread information. The default is Normal logging. Use Diagnostic only if you are troubleshooting a problem with GroupWise WebAccess.

   The verbose and diagnostic logging levels do not degrade WebAccess Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

   File Logging: Turns disk logging on or off. When disk logging is turned on, the WebAccess Agent creates a new log file each day and each time it is restarted. The log file is named *mmdd*web.*nnn*, where *mm* is the month, *dd* is the day, and *nnn* is a sequenced number (001 for the first log file of the day, 002 for the second, and so forth). On NetWare and Windows, the default location for the log files is the *domain*\wpgate*webac65a*\000.prc directory. On Linux, the default location is /var/log/novell/groupwise/*domain.webac65*a/000.prc.

   Max Log File Age: Specifies the number of days you want the WebAccess Agent to retain old log files. The WebAccess Agent will retain the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.

   Max Log Disk Space: Specifies the maximum amount of disk space you want to use for log files. If the disk space limit is exceeded, the WebAccess Agent will delete log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 65536 KB.

2. Press Esc to save the information.

Modifying Log Settings through the Windows Agent's Console

You can use the Windows WebAccess Agent's console to modify the logging level. All other log settings must be modified through ConsoleOne or startup switches. See "Modifying Log Settings in ConsoleOne" on page 833 and "Modifying Log Settings through Startup Switches" on page 834.

Changes you make to the log level at the console apply only to the current session. When you restart the WebAccess Agent, the log level is reset to the level specified in ConsoleOne or the startup switches.

To modify the logging level:

1 In the NetWare WebAccess Agent's console (the DOS window), press F2 to cycle the log level between Normal, Verbose, and Diagnostic. Each level is described below:

   Normal: Normal displays initial statistics, user logins, warnings, and errors. This is the default level.

   Verbose: Verbose displays Normal logging plus user requests.

   Diagnostic: Diagnostic displays Verbose logging plus thread information. Use Diagnostic only if you are troubleshooting a problem with GroupWise WebAccess.

   The verbose and diagnostic logging levels do not degrade WebAccess Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Modifying Log Settings on Linux

On Linux, these settings must be modified through ConsoleOne. See "Modifying Log Settings in ConsoleOne" on page 833.

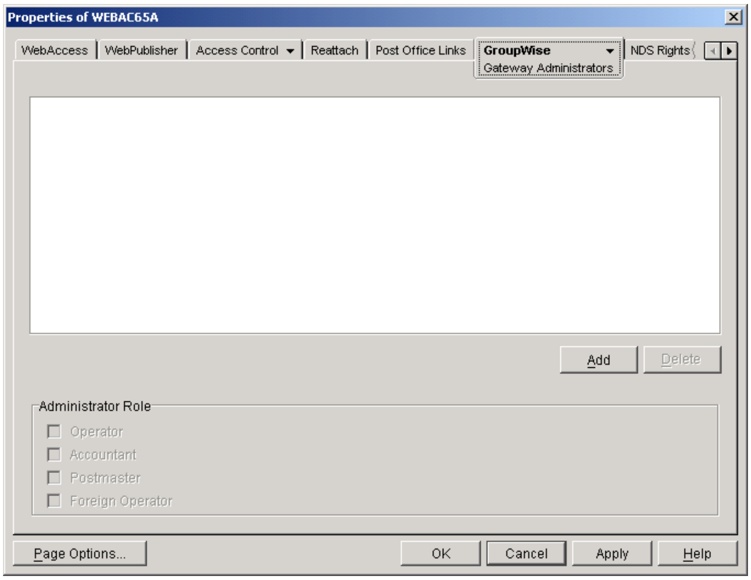
Assigning Operators to Receive Warning and Error Messages

You can select GroupWise users to receive warning and error messages issued by the WebAccess Agent. Whenever the agent issues a warning or error, these users, called operators, receive a message in their mailboxes. You can specify one or more operators.

To assign an operator:

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

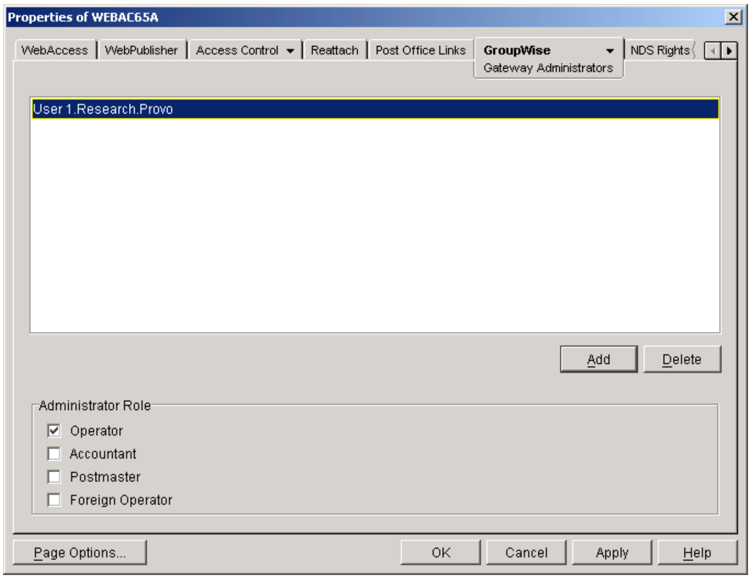
2 Click GroupWise > Gateway Administrators to display the Gateway Administrators page.



Administrator Role

- □ Operator
- □ Accountant
- □ Postmaster
- □ Foreign Operator

3 Click Add, select a user, then click OK to add the user to the Gateway Administrators list.



User 1.Research.Provo

Administrator Role

- ☑ Operator
- □ Accountant
- □ Postmaster
- □ Foreign Operator

4 Make sure Operator is selected as the Administrator Role.

5 If desired, add additional operators.

6 Click OK.

Managing Access to Post Offices

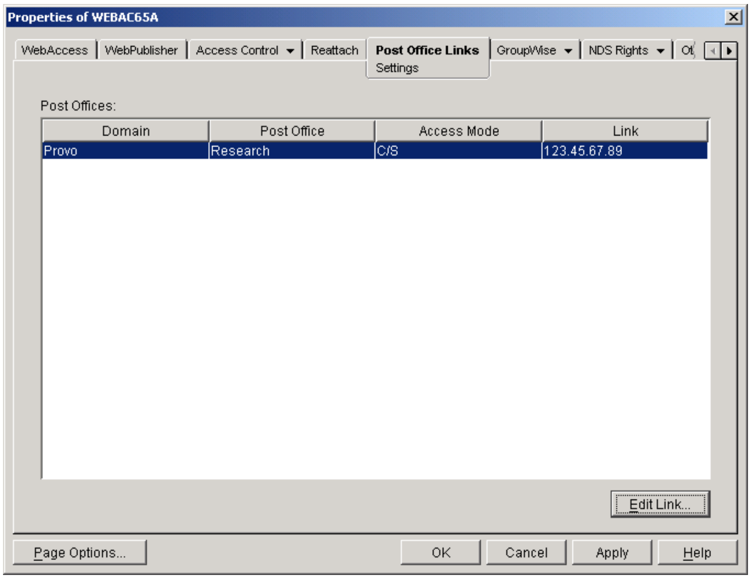
The WebAccess Agent requires access to all post offices where WebAccess users' mailboxes or GroupWise libraries reside. The agent can access a post office using client/server mode, direct mode, or both. By default, it uses whichever mode is defined on the Post Office object's Post Office Settings page (located on the GroupWise tab).

- "Modifying Links to Post Offices" on page 838 explains how to set the access mode to client/server, direct, or both.
- "Automating Reattachment to NetWare Servers" on page 839 explains how to configure the agent to automatically reconnect to post offices on NetWare servers.

Modifying Links to Post Offices

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

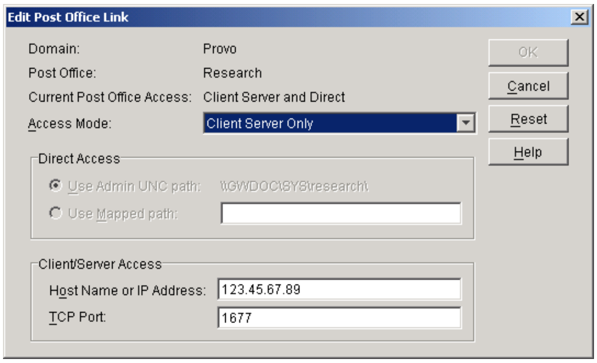
2 Click Post Office Links > Settings.



Post Offices:

Domain	Post Office	Access Mode	Link
Provo	Research	C/S	123.45.67.89

3 In the Post Offices list, select the post office whose link information you want to change, then click Edit Link to display the Edit Post Office Link dialog box.



Domain: Provo
Post Office: Research
Current Post Office Access: Client Server and Direct
Access Mode: Client Server Only

Direct Access
● Use Admin UNC path: \\GWDOC\SYS\research\
○ Use Mapped path:

Client/Server Access
Host Name or IP Address: 123.45.67.89
TCP Port: 1677

4 Define the following properties:

Access Mode: The access mode determines whether the WebAccess Agent will use client/server access, direct access, or both client/server and direct access to connect to the post office. With client/server and direct, the WebAccess Agent first tries client/server access; if client/server access fails, it then tries direct access. You can also choose to use the same access mode currently defined for the post office (on the Post Office object's Post Office Settings page). The current access mode is displayed in the Current Post Office Access field.

Direct Access: When connecting to the post office in direct mode, the WebAccess Agent can use the post office's UNC path (as defined on the Post Office object's Identification page) or a mapped path that you enter.

Client/Server Access: When connecting to the post office in client/server mode, the WebAccess Agent must know the hostname (or IP address) and port number of the Post Office Agent running against the post office.

5 Click OK.

6 Repeat Step 3 through Step 5 for each post office whose link you want to change.

Automating Reattachment to NetWare Servers

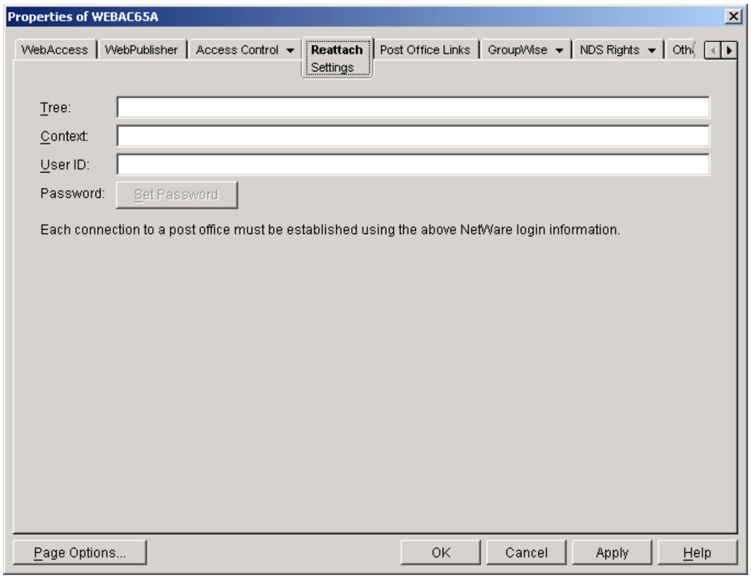
You can specify the reattach information for the Windows WebAccess Agent in ConsoleOne. Whenever the Windows WebAccess Agent loses its connection to a post office that is on a NetWare server, it will read the reattach information from the domain database and attempt to reattach to the NetWare server.

The NetWare WebAccess Agent does not use this information. To reattach to NetWare servers where users’ post offices reside, the NetWare WebAccess Agent uses the user ID and password specified during installation. This user ID and password are entered in the strtweb.ncf file

To specify the reattachment information for the NetWare WebAccess Agent:

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

2 Click Reattach > Settings.



Each connection to a post office must be established using the above NetWare login information.

3 Define the following properties:

Tree: Enter the eDirectory tree that the WebAccess Agent logs in to. If the WebAccess Agent does not use an eDirectory user account, leave this field blank.

Context: Enter the eDirectory context of the WebAccess Agent’s user account. If the WebAccess Agent does not use an eDirectory user account, leave this field blank.

User ID: Enter the name of the user account.

Password: Enter the password for the user account.

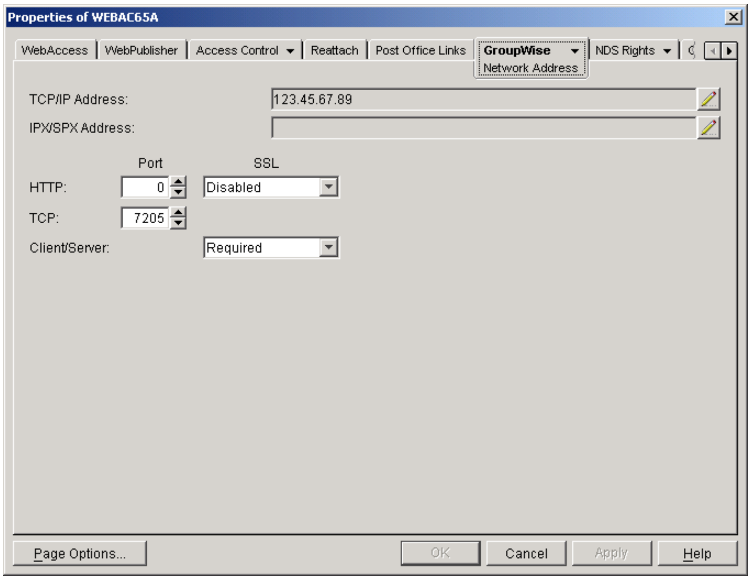
4 Click OK.

Changing the WebAccess Agent’s Network Address or Port Numbers

If you change the network address (IP address or DNS hostname) of the WebAccess Agent’s server or move the WebAccess Agent to a new server, you will need to change the network address in ConsoleOne. You can also change the port numbers used by the WebAccess Agent.

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

2 Click GroupWise > Network Address to display the Network Address page.



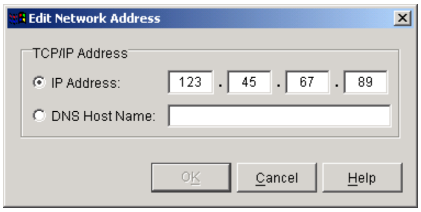
Properties of WEBAC65A

TCP/IP Address: 123.45.67.89

IPX/SPX Address:

	Port	SSL
HTTP:	0	Disabled
TCP:	7205	
Client/Server:		Required

3 To change the WebAccess Agent’s IP address, click the Edit button next to the TCP/IP Address field to display the Edit Network Address dialog box.



Edit Network Address

TCP/IP Address

● IP Address: 123 . 45 . 67 . 89

○ DNS Host Name:

4 Change the IP address or DNS hostname as necessary, then click OK to return to the Network Address page.

5 To change the port numbers used by the WebAccess Agent, enter the new port number in the appropriate field.

HTTP Port: This is the port used to listen for requests from its Web console. The default port number is 7211.

TCP Port: This is the port used to listen for requests from the WebAccess Application and WebPublisher Application. The default port is 7205.

6 Click OK to save the changes.

Configuring the WebAccess Application

During installation, the WebAccess Application is set up with a default configuration. However, you can use the information in the following sections to optimize the WebAccess Application configuration:

- "Modifying the WebAccess Application Environment Settings" on page 841
- "Controlling WebAccess Application Logging" on page 842
- "Adding or Removing Service Providers" on page 844
- "Modifying WebAccess Application Template Settings" on page 845
- "Securing WebAccess Application Sessions" on page 850
- "Controlling Availability of WebAccess Features" on page 852

Modifying the WebAccess Application Environment Settings

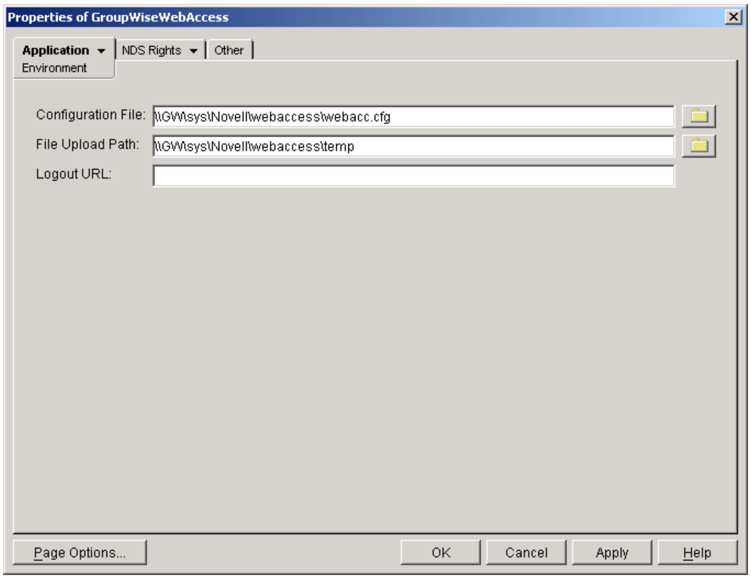
Using ConsoleOne®, you can modify the WebAccess Application's environment settings. The environment settings determine such things as the location where ConsoleOne stores the WebAccess Application's configuration file and how long the WebAccess Application will maintain an open session with an inactive user.

To modify the environment settings:

1 In ConsoleOne, right-click the WebAccess Application object (GroupWiseWebAccess), then click Properties.

NOTE: The WebAccess Application object is not available in the GroupWise View. To locate the WebAccess Application object, you must use the Console View.

2 If necessary, click Applications > Environment to display the Environment page.



Configuration File: \\GW\sys\Novell\webaccess\webacc.cfg

File Upload Path: \\GW\sys\Novell\webaccess\temp

Logout URL:

3 Modify any of the following fields:

Configuration File: The WebAccess Application does not have access to Novell® eDirectory™ or the GroupWise® domain database. Therefore, ConsoleOne writes the application's configuration information to the file specified in this field. By default, this is the webacc.cfg file located in the WebAccess Application's home directory (novell\webaccess on the Web server or /opt/novell/groupwise/webaccess on Linux).

In general, you should avoid changing the location of the file. If you do, you need to make sure to modify the webacc.cfg path in the Java* servlet engine's property file or (web.xml for Tomcat or servlets.properties for the Novell Servlet Gateway). If you do not, the WebAccess Application will continue to look for its configuration information in the old location.

File Upload Path: When a user attaches a file to an item, the file is uploaded to the directory displayed in this field. By uploading the file before the item is sent, less time is required to send the item when the user clicks the Send button. After the user sends the item (or cancels it), the WebAccess Application deletes the file from the directory.

Specify the upload directory you want to use. The default path is to the temp directory, located in the WebAccess Application's home directory (by default, novell\webaccess\temp on the Web server or /opt/novell/groupwise/webaccess/temp on Linux).

Logout URL: By default, users who log out of GroupWise WebAccess are returned to the login page. If desired, you can enter the URL for a different page.

The logout URL can be defined in this location and two additional locations. These locations are listed below, in the order that the WebAccess Application will check them.

- Trusted server logout URL (configured on the Security page)
- Template-specific logout URL (configured on the Templates page)
- General logout URL (configured on the Environment page)

For example, you define a general logout URL (WebAccess Application object > Environment page) and a Standard HTML template logout URL (WebAccess Application object > Templates page). You are not using trusted servers, so you do not set any trusted server logout URLs.

When a Standard HTML template user logs out of WebAccess, the Standard HTML template logout URL is used. However, when a Basic HTML template user logs out, the general logout URL is used.

If none of these locations include a logout URL, the WebAccess Application defaults to the standard login page.

4 Click OK to save the changes.

Controlling WebAccess Application Logging

The WebAccess Application logs information to log files on disk. You can control the following logging features:

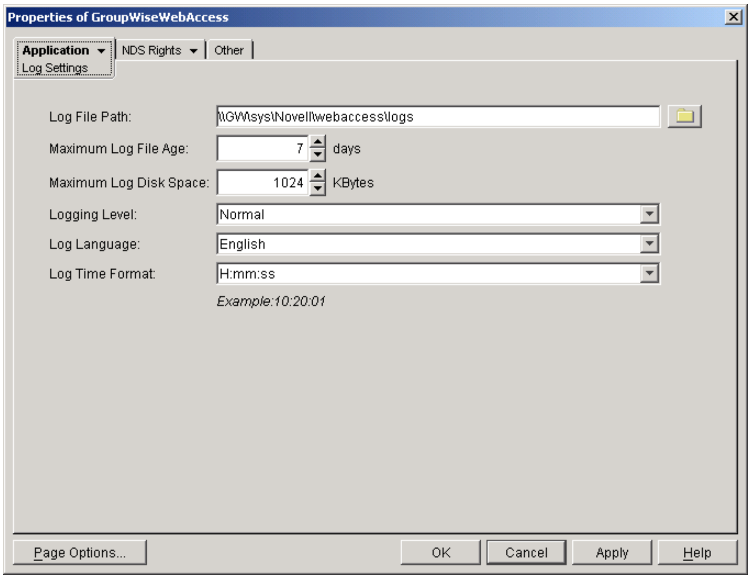
- The type of information to log
- How long to retain log files
- The maximum amount of disk space to use for log files
- Where to store log files

The WebAccess Application creates a new log file each day and each time it is restarted (as part of the Web server startup). The log file is named *mmdd*was.*nnn*, where *mm* is the month, *dd* is the year, and *nnn* is a sequenced log file number (001 for the first log file of the day, 002 for the second, and so forth).

To modify the log settings:

1 In ConsoleOne, right-click the WebAccess Application object, then click Properties.

2 Click Application > Log Settings to display the Log Settings page.



Log File Path: \\GW\sys\Novell\webaccess\logs

Maximum Log File Age: 7 days

Maximum Log Disk Space: 1024 KBytes

Logging Level: Normal

Log Language: English

Log Time Format: H:mm:ss

Example:10:20:01

3 Modify any of the following properties:

Log File Path: Specify the path to the directory where you want to store the log files.

On NetWare and Windows, the log files are stored in the novell\webaccess\logs directory on the Web server by default. On Linux, they are stored in /opt/novell/groupwise/webaccess/logs.

Maximum Log File Age: Specify the number of days you want to retain the log files. The WebAccess Application will retain the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.

Maximum Log Disk Space: Specify the maximum amount of disk space you want to use for the log files. If the disk space limit is exceeded, the WebAccess Application will delete log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 1024 KB.

Logging Level: There are four logging levels: None, Normal, Verbose, and Diagnostic. None turns logging off; Normal displays warnings and errors; Verbose displays Normal logging plus information messages and user requests; and Diagnostic displays all possible information. The default is Normal logging. Use Diagnostic only if you are troubleshooting a problem with WebAccess.

The verbose and diagnostic logging levels do not degrade WebAccess Application performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Log Language: Select the language in which you want information written to the log files. The list contains many languages, some of which the WebAccess Application might not support. If you select an unsupported language, the information will be written in English.

Log Time Format: Choose from the following formats to use when the WebAccess Application records dates and times in the log files: HH:mm:ss:SS, MM/dd: H:mm:ss.SS, or dd/MM: H:mm:ss.SS. H and HH represent hours, mm represents minutes, ss and SS represent seconds, MM represents months, and dd represents days.

4 Click OK to save the log settings.

Adding or Removing Service Providers

The WebAccess Application receives requests from users and then passes the requests to the appropriate service provider. The service provider fills the requests and returns the required information to the WebAccess Application. The WebAccess Application merges the information into the appropriate template and displays it to the user.

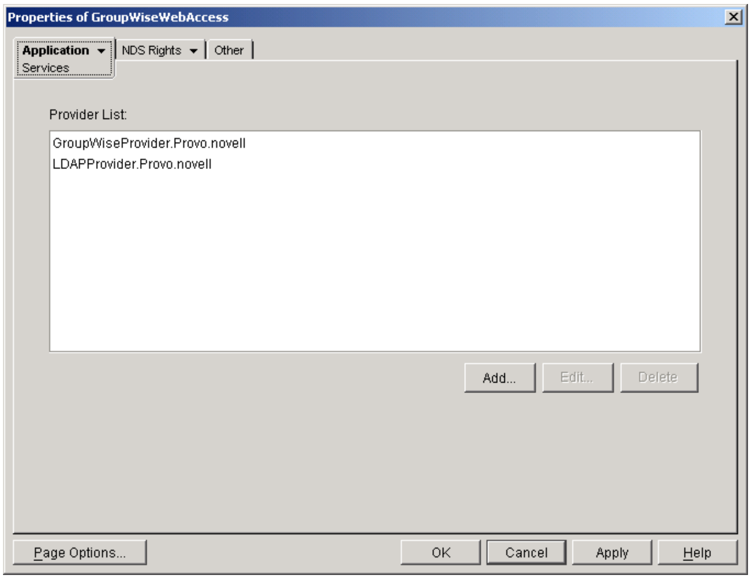
To function properly, the WebAccess Application must know which service providers are available. On NetWare and Windows, WebAccess includes two service providers: a GroupWise service provider (GroupWiseProvider) and an LDAP service provider (LDAPProvider). On Linux, there is also a separate GroupWiseDocumentProvider for WebPublisher. The GroupWise provider communicates with the WebAccess Agent to fill GroupWise requests. The LDAP provider communicates with LDAP servers to fill LDAP requests, such as LDAP directory searches initiated through the GroupWise Address Book.

Both the GroupWise service provider and the LDAP service provider are installed and configured at the same time as the WebAccess Application. You can disable the GroupWise service or LDAP service by removing the GroupWise service provider or LDAP service provider. On Linux, the GroupWiseDocumentProvider is also created by default. If you've created new service providers to expose additional services through GroupWise WebAccess, you must define those service providers so that the WebAccess Application knows about them.

To define service providers:

1. In ConsoleOne, right-click the WebAccess Application object, then click Properties.
2. Click Application > Services to display the Services page.

   The Provider List displays all service providers that the WebAccess Application is configured to use.



Provider List:

GroupWiseProvider.Provo.novell
LDAPProvider.Provo.novell

3. Choose from the following options:

   Add: To add a service provider to the list, click Add, browse for and select the service provider's object, then click OK.

   Edit: To edit a service provider's information, select the provider in the list, then click Edit. For information about the modifications you can make, see Chapter , "Configuring the

GroupWise Service Provider," on page 867 and Chapter , "Configuring the LDAP Service Provider," on page 868.

Delete: To remove a service provider from the list, select the provider, then click Delete.

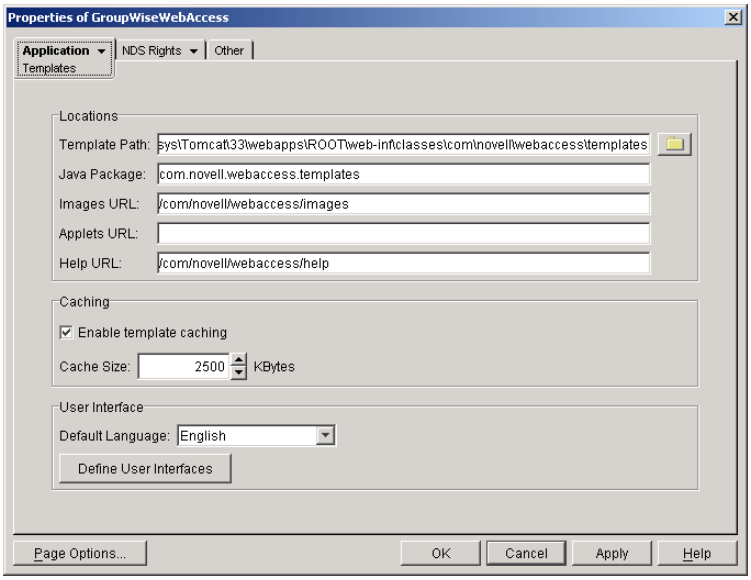
4 Click OK to save the changes.

Modifying WebAccess Application Template Settings

When the WebAccess Application receives information from a service provider, it merges the information into the appropriate WebAccess template before displaying the information to the user. Using ConsoleOne, you can modify the WebAccess Application's template settings. The template settings determine such things as the location of the templates, the maximum amount of server memory to use for caching the templates, and the default template language.

1 In ConsoleOne, right-click the WebAccess Application object, then click Properties.

2 Click Application > Templates to display the Templates page.



Properties of GroupWiseWebAccess

Locations

Template Path: sys\Tomcat\33\webapps\ROOT\web-inf\classes\com\novell\webaccess\templates

Java Package: com.novell.webaccess.templates

Images URL: /com/novell/webaccess/images

Applets URL:

Help URL: /com/novell/webaccess/help

Caching

☑ Enable template caching

Cache Size: 2500 KBytes

User Interface

Default Language: English

3 Modify any of the following fields:

Template Path: Select the location of the template base directory. The template base directory contains the subdirectories (simple, frames, hdml, and wml) for each of the templates provided with GroupWise WebAccess. If you create your own templates, you need to place the templates in a new subdirectory in the template base directory.

On a NetWare® server with the Novell Servlet Gateway, the default installation directory is java\servlets\com\novell\webaccess\templates.

On a Windows server with the Novell Servlet Gateway, the default installation directory is novell\java\servlets\com\novell\webaccess\templates.

On a NetWare or Windows server with Tomcat, the default installation directory is *tomcat_dir*\webapps\ROOT\web-inf\classes\com\novell\webaccess\templates.

On a Linux server with Tomcat, the default installation directory is /var/opt/novell/tomcat/webapps/gw/WEB-INF/classes/com/novell/webaccess/templates.

Java Package: Specify the Java package that contains the template resources used by the WebAccess Application. The default package is com.novell.webaccess.templates.

Images URL: Specify the URL for the GroupWise WebAccess image files. These images are merged into the templates along with the GroupWise information. This URL must be relative to the Web server's document root directory. On NetWare and Windows, the default relative URL is /com/novell/webaccess/images. On Linux, the default relative URL is /gw/com/novell/webaccess/images.

Applets URL: In some instances (Address Book and Month Calendar, for example), applets can be used instead of the standard templates. Specify the URL for the GroupWise WebAccess applets (Address Book, Month Calendar, and so forth). This URL must be relative to the Web server's document root directory. On NetWare and Windows, the default relative URL is /com/novell/webaccess/applets. On Linux, the default relative URL is /gw/com/novell/webaccess/applets.

Help URL: Specify the URL for the GroupWise WebAccess Help files. This URL must be relative to the Web server's document root directory. On NetWare and Windows, the default relative URL is /com/novell/webaccess/help. On Linux, the default relative URL is /gw/com/novell/webaccess/help.

Enable Template Caching: To speed up access to the template files, the WebAccess Application can cache the files to the server's memory. Select this option to turn on template caching.

Cache Size: Select the maximum amount of memory, in kilobytes, you want to use when caching the templates. The default cache size, 2500 KB, is sufficient to cache all templates shipped with GroupWise WebAccess. If you modify or add templates, you can turn on Verbose logging (WebAccess Application object > Application tab > Log Settings page) to view the size of the template files. Using this information, you can then change the cache size appropriately.

Default Language: If you have more than one language installed, select the language to use when displaying the initial GroupWise WebAccess page. If users want the GroupWise WebAccess interface (templates) displayed in a different language, they can change it on the initial page.

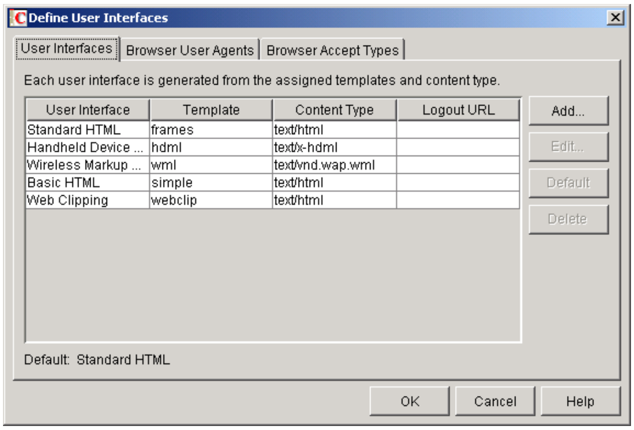
Define User Interfaces: GroupWise WebAccess supports Web browsers on many different devices (for example, computers and wireless telephones). Each device supports specific content types such as HTML, HDML, and WML. When returning information to a device's Web browser, the WebAccess Application must merge the information into a set of templates to create an interface that supports the content type required by the Web browser.

GroupWise WebAccess ships with five predefined user interfaces (Standard HTML, Basic HTML, Handheld Device Markup Language, Wireless Markup Language, and Web Clipping). These interfaces support Web browsers that require HTML, HDML, and WML content types. Click the User Interface button to view, add, modify, or delete user interfaces. For more information, see Defining User Interfaces below.

4 Click OK to save the changes.

Defining User Interfaces

1 From the WebAccess Application object's Templates page, click Define User Interfaces to display the Define User Interfaces dialog box.



Each user interface is generated from the assigned templates and content type.

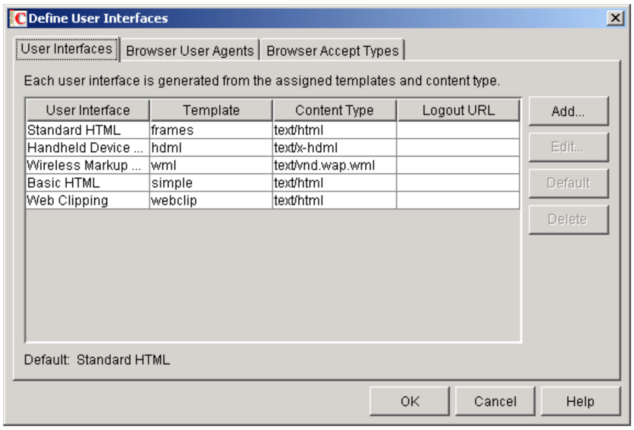
User Interface	Template	Content Type	Logout URL
Standard HTML	frames	text/html	
Handheld Device ...	hdml	text/x-hdml	
Wireless Markup ...	wml	text/vnd.wap.wml	
Basic HTML	simple	text/html	
Web Clipping	webclip	text/html	

Default: Standard HTML

The dialog box includes three tabs:

- **User Interfaces:** The User Interfaces tab lets you add, modify, and remove user interfaces, as well as determine whether or not GroupWise data added to an interface should be cached on proxy servers. Each interface consists of template files that support a specific content type. For example, the predefined Standard HTML interface uses frame-based HTML templates, located in the frames directory, that support the text/html content type.
- **Browser User Agents:** The Browser User Agents tab lets you associate a user interface with a Web browser. The association is based on the browser's User Agent information (signature, platform, version, and so forth). For example, if a browser's User Agent information includes "Windows CE" (one of the predefined entries), the WebAccess Application will use the Basic HTML interface (no-frames interface).
- **Browser Accept Types:** The Browser Accept Types tab lets you associate a user interface with a Web browser. The association is based on the content type the browser will accept. For example, if a browser accepts text/html (one of the predefined entries), the WebAccess Application will use the Standard HTML interface (frames-based interface).

2 To add, remove, or modify user interfaces, click the User Interfaces tab.



Each user interface is generated from the assigned templates and content type.

User Interface	Template	Content Type	Logout URL
Standard HTML	frames	text/html	
Handheld Device ...	hdml	text/x-hdml	
Wireless Markup ...	wml	text/vnd.wap.wml	
Basic HTML	simple	text/html	
Web Clipping	webclip	text/html	

Default: Standard HTML

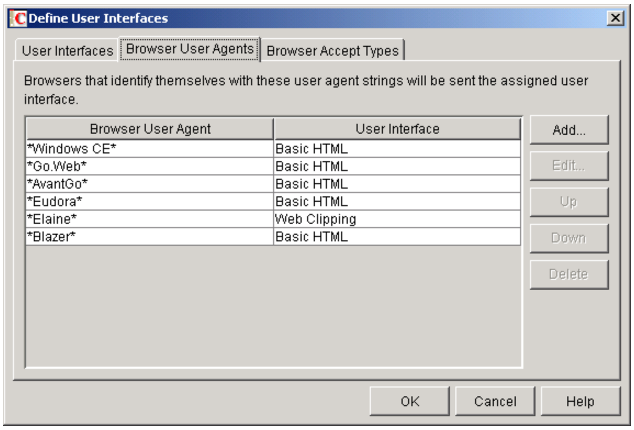
The User Interface list displays all available user interfaces. The list includes the following information:

- **User Interface:** This column displays the name assigned to the user interface (for example, Standard HTML or Wireless Markup Language).
- **Template:** This column displays the directory in which the template files are located. Only the directory name is shown. You can append this directory name to the template path shown on the Templates page to see the full template directory path.
- **Content Type:** This column displays the content type required by the templates (for example, text/html, text/x-hdml, or text/vnd.wap.wml).
- **Logout URL:** By default, when a user logs out, he or she is returned to the standard login page. When adding or editing the user interface, you can use the logout URL to define a different page. If you do so, this column displays the URL. This URL overrides the logout URL specified on the WebAccess Application object's Environment page (see "Modifying the WebAccess Application Environment Settings" on page 841). It is overridden by the logout URL specified for a trusted server on the WebAccess Application object's Security page (see "Securing WebAccess Application Sessions" on page 850).

Choose from the following options to manage the user interfaces:

- **Add:** Click Add to add a user interface to the list.
- **Edit:** Select a user interface in the list, then click Edit to edit the interface's name, template directory, content type, or proxy caching setting.
- **Default:** Select a user interface in the list, then click Default to make that interface the default interface. The WebAccess Application will use the default interface only if it can't determine the appropriate interface based on the browser's User Agent (Browser User Agent tab) or the browser's accepted content types (Browser Accept Types tab).
- **Delete:** Select a user interface in the list, then click Delete to remove the interface. This only removes the entry from the list. It does not delete the template files from the template directory.

3 To associate a user interface with a Web browser based on the browser's User Agent information, click the Browser User Agents tab.



Browsers that identify themselves with these user agent strings will be sent the assigned user interface.

Browser User Agent	User Interface
Windows CE	Basic HTML
Go.Web	Basic HTML
AvantGo	Basic HTML
Eudora	Basic HTML
Elaine	Web Clipping
Blazer	Basic HTML

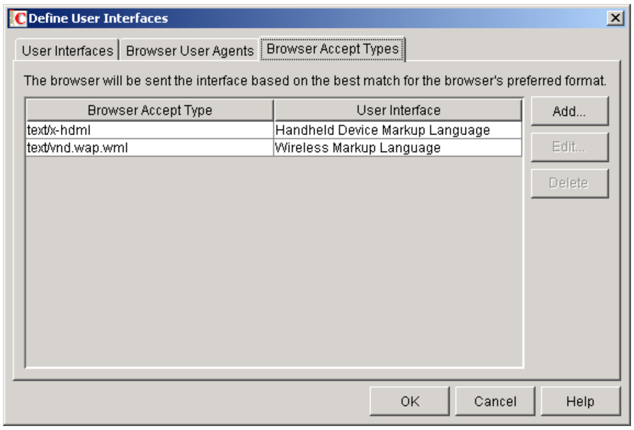
The Browser User Agents tab lets you associate a user interface with a Web browser. The association is based on the browser's User Agent information (signature, platform, version, and so forth). For example, if a browser's User Agent information includes "Windows CE" (one of the predefined entries), the WebAccess Application will use the Basic HTML interface (no-frames interface).

If a browser's User Agent information matches more than one entry in the list, the application uses the first entry. If the browser's User Agent information does not match any entries in the list, the WebAccess Application tries to select an interface based on the content types the browser will accept (Browser Accept Types tab). If no match is made based on the Accept Types information, the WebAccess Application uses the default user interface listed on the User Interfaces tab.

Choose from the following options to manage the associations:

- **Add:** Click Add to add an entry to the list.
- **Edit:** Select an entry from the list, then click Edit to edit the entry's information.
- **Up:** Select an entry from the list, then click Up to move it up in the list. If two entries match the information in a browser's User Agent header, the WebAccess Application uses the interface associated with the first entry listed.
- **Down:** Select an entry from the list, then click Down to move it down in the list.
- **Delete:** Select an entry from the list, then click Delete to remove the entry.

4 To associate a user interface with a Web browser based on the content type that the browser will accept, click the Browser Accept Types tab.



The browser will be sent the interface based on the best match for the browser's preferred format.

Browser Accept Type	User Interface
text/x-hdml	Handheld Device Markup Language
text/vnd.wap.wml	Wireless Markup Language

The Browser Accept Types tab lets you associate a user interface with a Web browser. The association is based on the content type the browser will accept. For example, if a browser accepts text/html (one of the predefined entries), the WebAccess Application will use the Standard HTML interface (frames-based interface).

Many browsers accept more than one content type (for example, both text/html and text/plain). If the list contains more than one acceptable content type, the WebAccess Application uses the browser's preferred content type, which is the type that is listed first in the browser's Accept Type header.

If no interface can be determined based on the entries in the list, the WebAccess Application uses the default user interface listed on the User Interfaces tab.

Choose from the following options to manage the associations:

- **Add:** Click Add to add an entry to the list.
- **Edit:** Select an entry from the list, then click Edit to edit the entry's information.
- **Delete:** Select an entry from the list, then click Delete to remove the entry.

5 Click OK to save your changes and return to the WebAccess Application object's Templates page.

Securing WebAccess Application Sessions

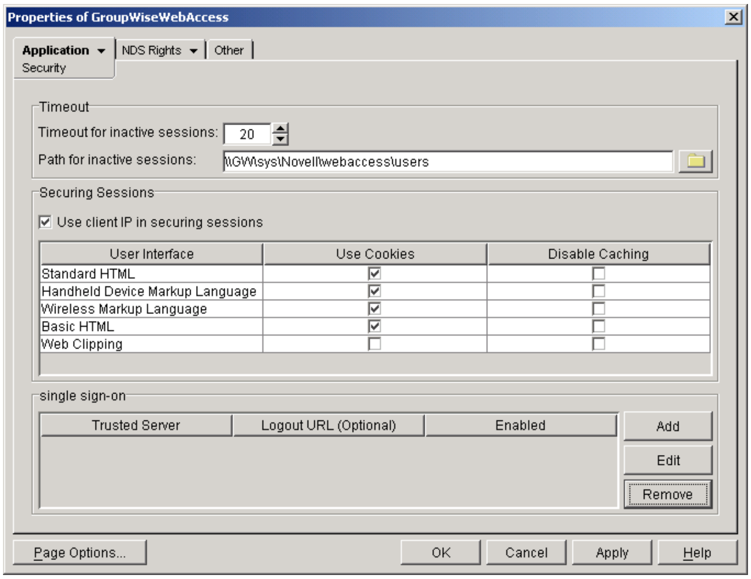
The WebAccess Application includes several settings to help you ensure that users' information is secure. You can:

- Specify a period of time after which inactive sessions will be closed. The default is 20 minutes.
- Secure sessions through the use of client IP binding or browser session cookies.
- Disable information caching by proxy servers and Web browsers.
- Enable GroupWise authentication through a trusted server.

To modify the security settings:

1 In ConsoleOne, right-click the WebAccess Application object, then click Properties.

2 Click Application > Security to display the Security page.



Timeout

Timeout for inactive sessions: 20

Path for inactive sessions: \\GW\sys\Novell\webaccess\users

Securing Sessions

☑ Use client IP in securing sessions

User Interface	Use Cookies	Disable Caching
Standard HTML	☑	□
Handheld Device Markup Language	☑	□
Wireless Markup Language	☑	□
Basic HTML	☑	□
Web Clipping	□	□

single sign-on

Trusted Server	Logout URL (Optional)	Enabled

3 Modify any of the following fields:

Timeout for Inactive Sessions: When a user logs in, the WebAccess Application opens a session with the user. This option lets you specify a period of time after which the WebAccess Application will close a session that has become inactive. A session becomes inactive when the user does not perform any actions, such as opening a message, that generate calls to the WebAccess Application. Having a timeout period not only provides security for users' e-mail but also ensures that GroupWise WebAccess runs efficiently.

Select how long the WebAccess Application should wait before ending an inactive session. If the user attempts to perform an action after the session has timed out, he or she will be prompted to log in again.

Path for Inactive Sessions: Browse for and select the folder where you want the WebAccess Application to save information about inactive sessions. This allows the WebAccess Application to return the user to the exact state he or she was in when the session timed out. Inactive sessions are automatically deleted after a period of time.

The default path is to the users directory, located in the WebAccess Application's home directory (by default, novell\webaccess\users on the Web server, or /opt/novell/groupwise/webaccess/users on Linux).

Use Client IP in Securing Sessions: Select this option if you want the WebAccess Application to bind the client IP address to the session. For that session, the WebAccess Application will accept requests from the bound IP address only. If you are using a proxy server that masks the client IP address, you should use the Use Cookies option instead.

User Interface/Use Cookies/Disable Caching: You can increase security by using session cookies and disabling caching of WebAccess information. Session cookies and caching are configurable on a per-user interface (template basis). For example, you could use session cookies and disable caching for the Standard HTML interface and not use session cookies or disable caching for the Wireless Markup Language interface.

- **Use Cookies:** Select this option if you want the WebAccess Application to use a session cookie to secure the user's session. The session cookie, which is created when the user opens the session, ties the session to the browser and ensures that the WebAccess Application will accept session requests from that browser only. The session cookie is held in memory and exists only as long as the user is logged in.

  By default, session cookies are enabled for all interfaces, with the exception of the Web Clippings interface, which does not support session cookies.

- **Disable Caching:** This option affects both Web browser caching and proxy server caching. Because the WebAccess Application sends sensitive mailbox information (such as message text and passwords) to users, caching of files by Web browsers and proxy servers can pose an information security risk.

  If you select the Disable Caching option, the WebAccess Application includes a "disable caching" request in the header of each file that it sends. By default, Web browsers honor this request and will not cache files that include the request. Proxy servers, on the other hand, might or might not honor the request, depending on how they are configured. If the proxy server honors the request, the file will not be cached; if it does not honor the request, the file will be cached, regardless of this setting.

Single Sign-On: The WebAccess Application supports authentication to GroupWise using Base64 authentication header credentials generated by a trusted server (for example, a Novell® iChain® Authentication Server). The authentication header generated by the trusted server must contain the username and password required to log the user into GroupWise. For this to occur, one of the following conditions must be met:

- The regular GroupWise username and password must match the credentials passed from the trusted server.

  or

- The LDAP authentication credentials used by each POA (if LDAP has been enabled) must match the credentials passed from the trusted server (ConsoleOne > Post Office object > GroupWise tab > Security page).

If the credentials passed from the trusted server match the credentials being used by the GroupWise system, then the GroupWise WebAccess login page is bypassed and the user has immediate access to the requested mailbox.

To specify a trusted server whose authentication header credentials will be accepted by the WebAccess Application, click Add to display the Add Trusted Server Information dialog box, then enter the server's IP address or DNS hostname. For more information about the fields in the Add Trusted Server Information dialog box, click the dialog box's Help button.

Controlling Availability of WebAccess Features

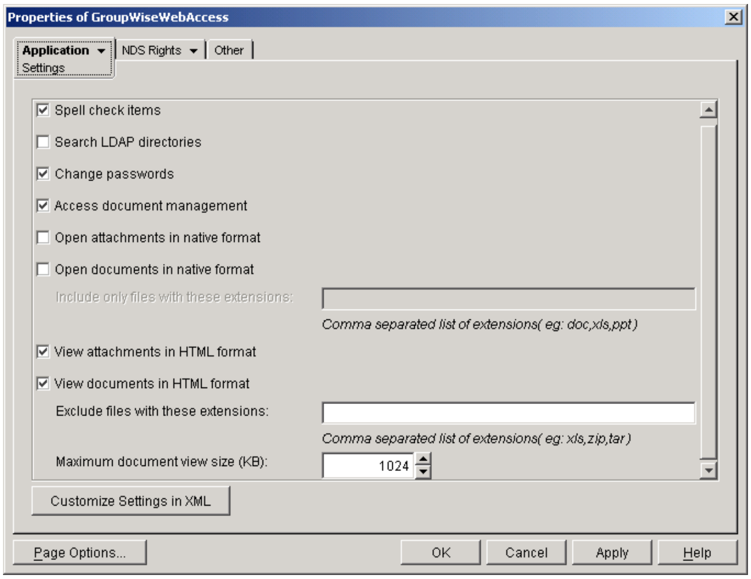
By default, WebAccess users can:

- Spell check messages
- Search LDAP directories (must be manually enabled on Linux)
- Change their GroupWise mailbox passwords
- Use Document Management Services
- Open attachments in native format (must be manually enabled on Linux)
- Open documents in native format (must be manually enabled on Linux)
- View attachments in HTML format
- View documents in HTML format

All users who log in through a single Web server will have the same feature access. You cannot configure individual user settings. However, if you have multiple Web servers, you can establish different settings for the Web servers by completing the following steps for each server's WebAccess Application.

To configure the WebAccess Application's user settings:

1. In ConsoleOne, right-click the WebAccess Application object, then click Properties.
2. Click Application > Settings to display the Settings page.



Properties of GroupWiseWebAccess

☑ Spell check items

☐ Search LDAP directories

☑ Change passwords

☑ Access document management

☐ Open attachments in native format

☐ Open documents in native format

Include only files with these extensions:

Comma separated list of extensions(eg: doc,xls,ppt)

☑ View attachments in HTML format

☑ View documents in HTML format

Exclude files with these extensions:

Comma separated list of extensions(eg: xls,zip,tar)

Maximum document view size (KB): 1024

3. Configure the following settings:

   Spell Check Items: Enable this option if you want users to be able to use the Novell Speller to spell check an item's text before sending the item. Disable this option to remove all Spell Check features from the user interface.

   Search LDAP Directories: Enable this option if you have an LDAP server and you want users to be able to search any LDAP address books you have defined. Disable this option to remove all LDAP features from the user interface.

Change Passwords: Enable this option if you want users to be able to change their Mailbox passwords. Disable this option to remove all Password features from the user interface.

Access Document Management: Enable this option if you want users to be able to use the Document Management features. Disable this option to remove all Document Management features from the user interface.

Open Attachments in Native Format: By default, the Save As option enables users to save message attachments to their local drives and then open them in their native applications. You can turn on this option to enable the Open option. The Open option enables users to open message attachments directly in their native applications without first saving the files to the local drive.

This option requires that 1) each user's Web browser knows the correct application or plug-in to associate with the attachment, according to its file extension or MIME type, and 2) the application or plug-in is available to the user. Otherwise, the user will be prompted to save the file to disk or specify the application to open it.

This option and the View Attachments in HTML Format option can both be enabled at the same time. Doing so gives users both the Open option and the View option, which means they have the choice of opening an attachment in its native application or viewing it as HTML.

Open Documents in Native Format: By default, the Save As option enables user to save library documents to their local drives and then open them in their native applications. You can turn on this option to enable the Open option. The Open option enables users to open documents directly in their native applications without first saving the files to the local drive.

This option requires that 1) each user's Web browser knows the correct application or plug-in to associate with the document, according to its file extension or MIME type, and 2) the application or plug-in is available to the user. Otherwise, the user will be prompted to save the file to disk or specify the application to open it.

This option and the View Documents in Native Format option can both be enabled at the same time. Doing so gives users both the Open option and the View option, which means they have the choice of opening a document in its native application or viewing it as HTML.

- **Include Only Files With These Extensions:** If you want only certain file types to be have the Open option, enter the file types in the Include Only Files With These Extensions field. Include only the extension and separate each extension with a comma (for example, doc, xls, ppt). The Open option will not be available for any file types not entered in this field. This setting applies when opening either library documents or attachments.

View Attachments in HTML Format: Enable this option if you want users to be able to view any type of attachments in HTML format. Disable this option to require users to save an attachment to a local drive and view it in its native application. WebAccess uses Stellent Outside In HTML Export to convert files to HTML format.

For a list of the supported file format conversions, download the following document from the Stellent Web site:

OutSide In Supported Platforms and File Formats (http://www.stellent.com/stellent3/groups/mkt/documents/nativepage/outside_in_supported_platforms.pdf)

This option and the Open Attachments in Native Format option can both be enabled at the same time. Doing so gives users both the View option and the Open option, which means they have the choice of viewing an attachment as HTML or opening it in its native application.

View Documents in HTML Format: Enable this option if you want users to be able to view library documents in HTML format. Disable this option to require users to save a document to a local drive and view it in its native application. WebAccess uses Stellent Outside In HTML Export to convert files to HTML format.

For a list of the supported file format conversions, download the following document from the Stellent Web site:

OutSide In Supported Platforms and File Formats (http://www.stellent.com/stellent3/groups/mkt/documents/nativepage/outside_in_supported_platforms.pdf)

This option and the Open Documents in Native Format option can both be enabled at the same time. Doing so gives users both the View option and the Open option, which means they have the choice of viewing a document as HTML or opening it in its native application.

- **Exclude Files With These Extensions:** If you want to exclude certain file types from having the View option, enter the file types in the Exclude Files With These Extensions field. Include only the extension and separate each extension with a comma (for example, doc, xls, ppt). The View option will be available for any file types not entered in this field. This setting applies when viewing either library documents or attachments.
- **Maximum Document View Size:** Specify the maximum size file that can be viewed in HTML format. If a file exceeds the maximum size, it must be opened in native format (if allowed) rather than viewed in HTML format. The default maximum size is 1024 KB. This setting applies when viewing either library documents or attachments.

4 Click OK.

Configuring the Novell Speller Application

The Novell® Speller Application enables users to spell check their messages. The Speller Application is installed automatically with the WebAccess Application. During installation, the Speller Application is set up with a default configuration. However, you can use the information in the following sections to optimize the Speller Application configuration:

- "Modifying the Speller Application Environment Settings" on page 854
- "Controlling Speller Application Logging" on page 855

Modifying the Speller Application Environment Settings

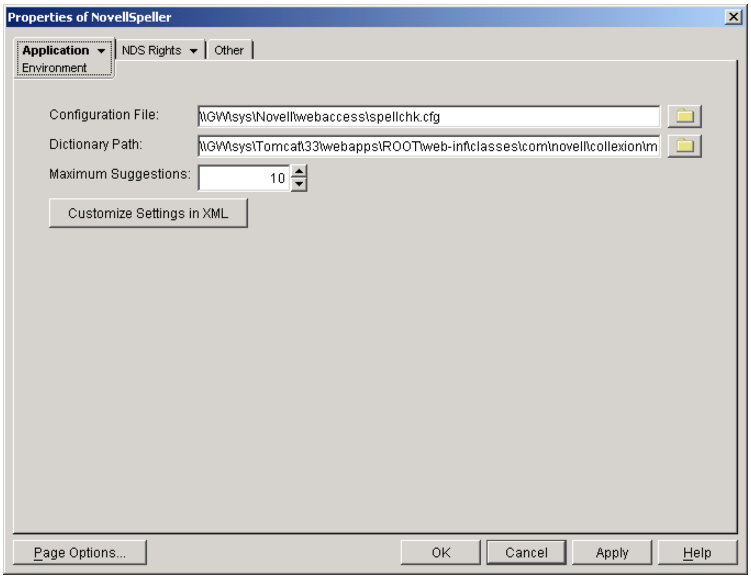
Using ConsoleOne®, you can modify the Speller Application's environment settings. The environment settings determine such things as the location where ConsoleOne stores the Speller Application's configuration file.

To modify the environment settings:

1 In ConsoleOne, right-click the Speller Application object (NovellSpeller), then click Properties.

NOTE: The Speller Application object is not available in the GroupWise View. To locate the Speller Application object, you must use the Console View.

2 If necessary, click Application > Environment to display the Environment page.



Properties of NovellSpeller

Configuration File: \\GW\sys\Novell\webaccess\spellchk.cfg

Dictionary Path: \\GW\sys\Tomcat\33\webapps\ROOT\web-inf\classes\com\novell\collexion\m

Maximum Suggestions: 10

3 Modify any of the following fields:

Configuration File: The Speller Application does not have access to Novell eDirectory™ or the GroupWise® domain database. Therefore, ConsoleOne writes the application's configuration information to the file specified in this field. By default, this is the spellchk.cfg file located in the WebAccess Application's home directory (novell\webaccess on the Web server or /opt/novell/groupwise/webaccess on Linux).

In general, you should avoid changing the location of the file. If you do change the location of the file, you need to make sure to modify the spellchk.cfg path in the Java servlet engine's properties file. If you do not, the Speller Application will continue to look for its configuration information in the old location.

Dictionary Path: Displays the path to the dictionary files used by the Speller Application.

On a NetWare® server with the Novell Servlet Gateway, the default installation directory is java\servlets\com\novell\collexion\morphology\data.

On a Windows server with the Novell Servlet Gateway, the default installation directory is novell\java\servlets\com\novell\collexion\morphology\data.

On a NetWare or Windows server with Tomcat, the default installation directory is *tomcat_dir*\webapps\ROOT\web-inf\classes\com\novell\collexion\morphology\data.

On Linux with Tomcat, the default installation directory is /var/opt/novell/tomcat/webapps/gw/WEB-INF/classes/com/novell/collexion/morphology/data.

Maximum Suggestions: Select the maximum number of suggestions the Speller Application will return for misspelled words. The default is 10.

Customize Settings in XML: Click this button to launch the XML editor. You can use the editor to add, modify, or delete settings.

4 Click OK to save the changes.

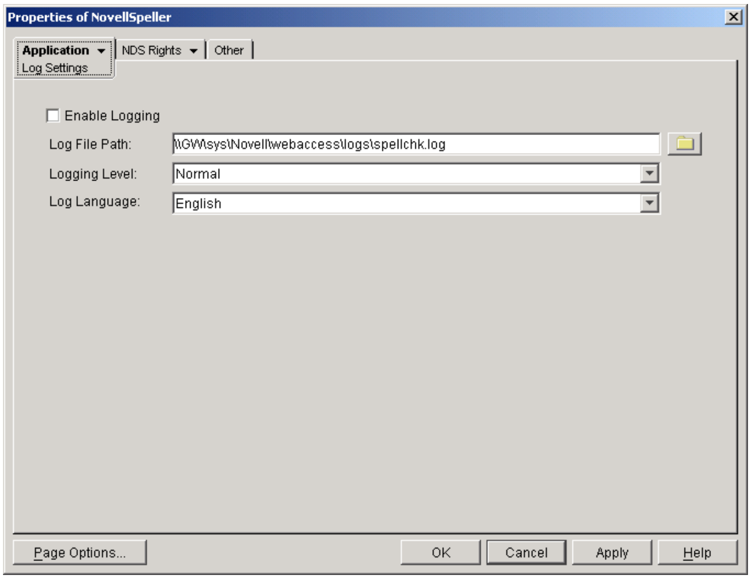
Controlling Speller Application Logging

The Speller Application can log information to a log file on disk. By default, logging is turned off. You can control the following logging features:

- Enable or disable logging
- Where to store the log file
- The type of information to log
- The language to use for the log file

To modify the log settings:

1. In ConsoleOne, right-click the Speller Application object, then click Properties.
2. Click Application > Log Settings to display the Log Settings page.



□ Enable Logging

Log File Path: \\GW\sys\Novell\webaccess\logs\spellchk.log

Logging Level: Normal

Log Language: English

3. Modify any of the following properties:

   Enable Logging: By default, logging is disabled. Select this option to enable it.

   Log File Path: Specify the path and filename for the log file.

   The log file is named spellchk.log by default. On NetWare and Windows, the log file is stored in the novell\webaccess\logs directory on the Web server by default. On Linux, the log file is stored in /opt/novell/groupwise/webaccess/logs.

   Logging Level: There are four logging levels: None, Normal, Verbose, and Diagnostic. None turns logging off; Normal displays warnings and errors; Verbose displays Normal logging plus information messages and user requests; and Diagnostic displays all possible information. The default is Normal logging. Use Diagnostic only if you are troubleshooting a problem with WebAccess.

   The verbose and diagnostic logging levels do not degrade Speller Application performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

   Log Language: Select the language in which you want information written to the log files. The list contains many languages, some of which the Speller Application might not support. If you select an unsupported language, the information will be written in English.

4. Click OK to save the log settings.

Configuring the WebPublisher Application

During installation, the WebPublisher Application is set up with a default configuration. However, you can use the information in the following sections to optimize the WebPublisher Application configuration:

- "Modifying the WebPublisher Application Environment Settings" on page 857
- "Controlling WebPublisher Application Logging" on page 858
- "Adding or Removing Service Providers" on page 859
- "Modifying WebPublisher Application Template Settings" on page 860
- "Controlling Availability of WebPublisher Features" on page 865

Modifying the WebPublisher Application Environment Settings

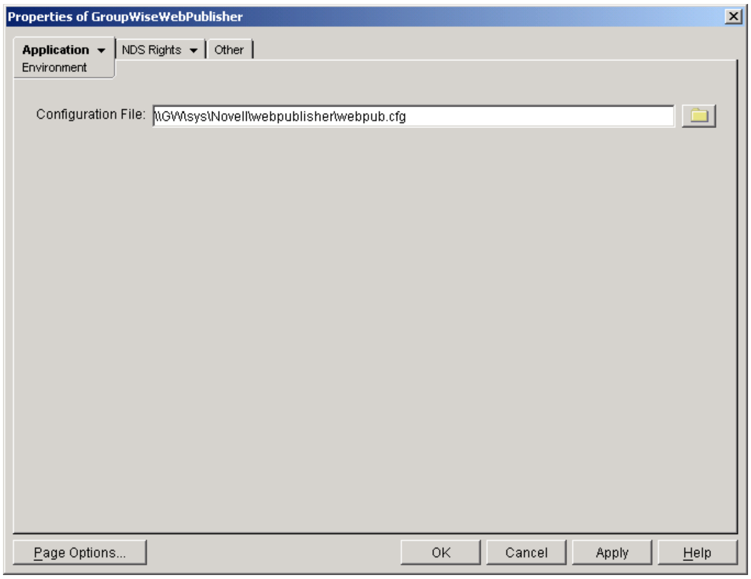
Using ConsoleOne®, you can modify the WebPublisher Application's environment settings. The environment settings determine such things as the location where ConsoleOne stores the WebPublisher Application's configuration file.

To modify the environment settings:

1 In ConsoleOne, right-click the WebPublisher Application object (GroupWiseWebPublisher), click Properties.

NOTE: The WebPublisher Application object is not available in the GroupWise View. To locate the WebPublisher Application object, you must use the Console View.

2 If necessary, click Application > Environment to display the Environment page.



Configuration File: \\GW\sys\Novell\webpublisher\webpub.cfg

3 Modify any of the following fields:

Configuration File: The WebPublisher Application does not have access to Novell® eDirectory™ or the GroupWise® domain database. Therefore, ConsoleOne writes the application's configuration information to the file specified in this field. By default, this is the webpub.cfg file located in the WebPublisher Application's home directory (novell\webpublisher on the Web server or /opt/novell/groupwise/webpublisher on Linux).

In general, you should avoid changing the location of the file. If you do change the location of the file, you need to make sure to modify the webpub.cfg path in the Java servlet engine's properties file. If you do not, the WebPublisher Application will continue to look for its configuration information in the old location.

4 Click OK to save the changes.

Controlling WebPublisher Application Logging

The WebPublisher Application logs information to log files on disk. You can control the following logging features:

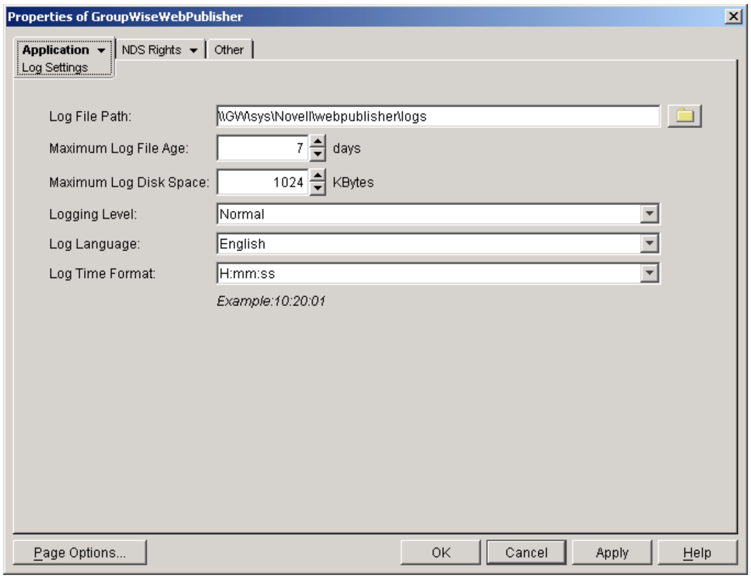
- The type of information to log
- How long to retain log files
- The maximum amount of disk space to use for log files
- Where to store log files

The WebPublisher Application creates a new log file each day and each time it is restarted (as part of the Web server startup). The log file is named *mmdd*wps.*nnn*, where *mm* is the month, *dd* is the year, and *nnn* is a sequenced log file number (001 for the first log file of the day, 002 for the second, and so forth).

To modify the log settings:

1 In ConsoleOne, right-click the WebPublisher Application object, then click Properties.

2 Click Application > Log Settings to display the Log Settings page.



Properties of GroupWiseWebPublisher

Log File Path: \\GW\sys\Novell\webpublisher\logs

Maximum Log File Age: 7 days

Maximum Log Disk Space: 1024 KBytes

Logging Level: Normal

Log Language: English

Log Time Format: H:mm:ss

Example:10:20:01

3 Modify any of the following properties:

Log File Path: Specify the path to the directory where you want to store the log files.

On NetWare and Windows, the log files are stored in the novell\webpublisher\logs directory on the Web server by default. On Linux, the log files are stored in /opt/novell/groupwise/webpublisher/logs.

Maximum Log File Age: Specify the number of days you want to retain the log files. The WebPublisher Application will retain the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.

Maximum Log Disk Space: Specify the maximum amount of disk space you want to use for the log files. If the disk space limit is exceeded, the WebPublisher Application will delete log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 1024 KB.

Logging Level: There are four logging levels: None, Normal, Verbose, and Diagnostic. None turns logging off; Normal displays warnings and errors; Verbose displays Normal logging plus information messages and user requests; and Diagnostic displays all possible information. The default is Normal logging. Use Diagnostic only if you are troubleshooting a problem with WebPublisher.

The verbose and diagnostic logging levels do not degrade WebPublisher Application performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Log Language: Select the language in which you want information written to the log files. The list contains many languages, some of which the WebPublisher Application might not support. If you select an unsupported language, the information will be written in English.

Log Time Format: Choose from the following formats to use when the WebPublisher Application records dates and times in the log files: HH:mm:ss:SS, MM/dd: H:mm:ss.SS, or dd/MM: H:mm:ss.SS. H and HH represent hours, mm represents minutes, ss and SS represent seconds, MM represents months, and dd represents days.

4 Click OK to save the log settings.

Adding or Removing Service Providers

The WebPublisher Application receives requests from users and then passes the requests to the appropriate service provider. The service provider fills the requests and returns the required information to the WebPublisher Application. The WebPublisher Application merges the information into the appropriate template and displays it to the user.

To function properly, the WebPublisher Application must know which service providers are available. By default, WebPublisher includes one service provider, the GroupWise Document service provider (GroupWiseDocumentProvider). The GroupWise Document service provider communicates with the WebAccess Agent to fill WebPublisher requests.

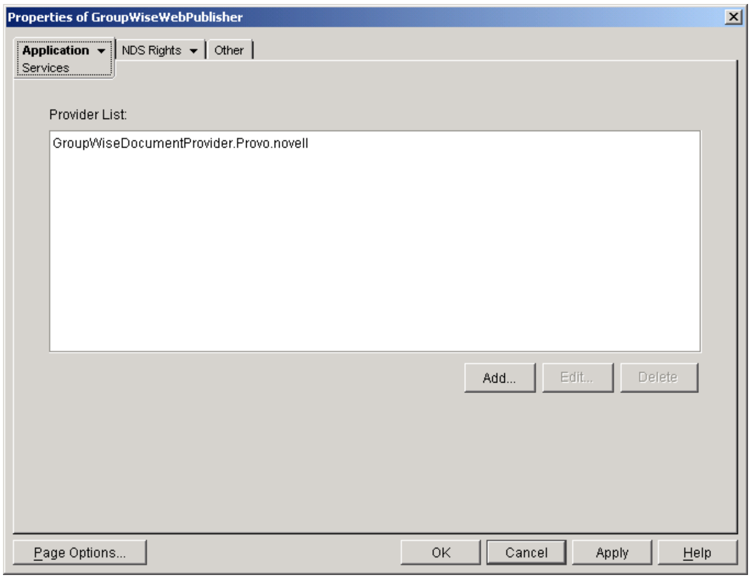
The GroupWise Document service provider is installed and configured at the same time as the WebPublisher Application. You can disable the GroupWise Document service by removing the GroupWise Document service provider. If you’ve created new service providers to expose additional services through GroupWise WebPublisher, you must define those service providers so that the WebPublisher Application knows about them.

To define service providers:

1 In ConsoleOne, right-click the WebPublisher Application object, then click Properties.

2 Click Application > Services to display the Services page.

The Provider List displays all service providers that the WebPublisher Application is configured to use.



Provider List:

GroupWiseDocumentProvider.Provo.novell

3 Choose from the following options:

Add: To add a service provider to the list, click Add, browse for and select the service provider's object, then click OK.

Edit: To edit a service provider's information, select the provider in the list, then click Edit. For information about the modifications you can make, see Chapter , "Configuring the GroupWise Document Service Provider," on page 869.

Delete: To remove a service provider from the list, select the provider > click Delete.

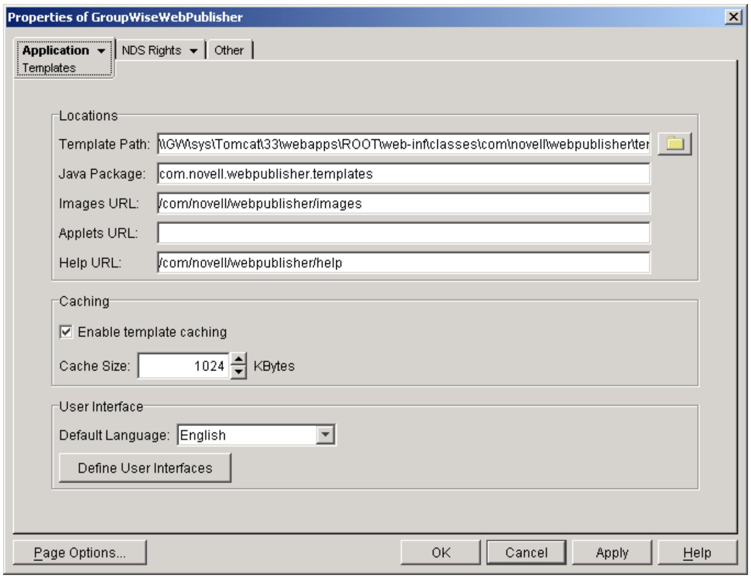
4 Click OK to save the changes.

Modifying WebPublisher Application Template Settings

When the WebPublisher Application receives information from a service provider, it merges the information into the appropriate WebPublisher template before displaying the information to the user. Using ConsoleOne, you can modify the WebPublisher Application's template settings. The template settings determine such things as the location of the templates, the maximum amount of server memory to use for caching the templates, and the default template language.

1 In ConsoleOne, right-click the WebPublisher Application object, then click Properties.

2 Click Application > Templates to display the Templates page.



Template Path: \\GW\sys\Tomcat\33\webapps\ROOT\web-inf\classes\com\novell\webpublisher\ter

Java Package: com.novell.webpublisher.templates

Images URL: /com/novell/webpublisher/images

Applets URL:

Help URL: /com/novell/webpublisher/help

☑ Enable template caching

Cache Size: 1024 KBytes

Default Language: English

3 Modify any of the following fields:

Template Path: Select the location of the template base directory. The template base directory contains the subdirectories for each of the templates provided with GroupWise WebAccess. Currently, only one template is provided for WebPublisher. This is an HTML template that uses frames; the template files are stored in the FRAMES subdirectory. If you create your own templates, you need to place the templates in a new subdirectory in the template base directory.

On a NetWare® server with the Novell Servlet Gateway, the default installation directory is java\servlets\com\novell\webpublisher\templates.

On a Windows server with the Novell Servlet Gateway, the default installation directory is novell\java\servlets\com\novell\webpublisher\templates.

On a NetWare or Windows server with Tomcat, the default installation directory is *tomcat_dir*\webapps\ROOT\web-inf\classes\com\novell\webpublisher\templates.

On a Linux server with Tomcat, the default installation directory is /var/opt/tomcat/webapps/gw/WEB-INF/classes/com/novell/webpublisher/templates.

Java Package: Specify the Java package that contains the template resources used by the WebPublisher Application. The default package is com.novell.webpublisher.templates.

Images URL: Specify the URL for the GroupWise WebPublisher image files. These images are merged into the templates along with the GroupWise document information. This URL must be relative to the Web server's document root directory. On NetWare and Windows, the default relative URL is /com/novell/webpublisher/images. On Linux, the default relative URL is /gw/com/novell/webpublisher/images.

Applets URL: GroupWise WebPublisher does not include any applets. If you create GroupWise WebPublisher applets, you need to specify the URL for the applets. To mirror the storage location of the GroupWise WebAccess applets, you can store the applets in a com\novell\webpublisher\applets directory under the Web server's document root directory. The applets URL would then be relative to the Web server's document root directory (for example, /com/novell/webpublisher/applets on NetWare or Windows, and /gw/com/novell/webpublisher/applets on Linux).

Help URL: Specify the URL for the GroupWise WebPublisher Help files. This URL must be relative to the Web server's document root directory. On NetWare and Windows, the default relative URL is /com/novell/webpublisher/help. On Linux, the default relative URL is /gw/com/novell/webpublisher/help.

Enable Template Caching: To speed up access to the template files, the WebPublisher Application can cache the files to the server's memory. Select this option to turn on template caching.

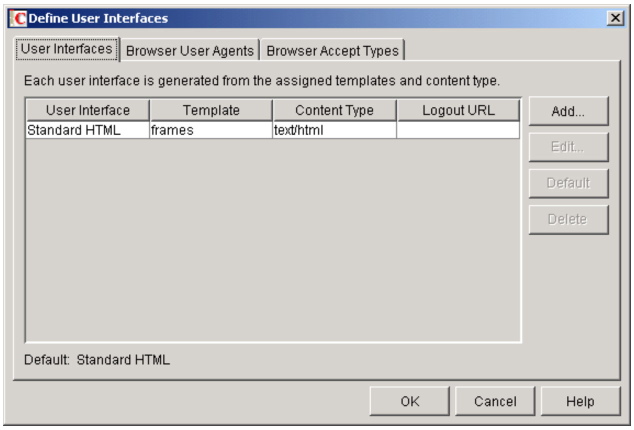
Cache Size: Select the maximum amount of memory, in kilobytes, you want to use when caching the templates. The default cache size, 1024 KB, is sufficient to cache all templates shipped with GroupWise WebPublisher. If you modify or add templates, you can turn on Verbose logging (WebPublisher Application object > Application tab > Log Settings page) to view the size of the template files. Using this information, you can then change the cache size appropriately.

Default Language: Select the language to use when displaying the initial GroupWise WebPublisher page. If users want the GroupWise WebPublisher interface (templates) displayed in a different language, they can change it on the initial page.

4 Click OK to save the changes.

Defining User Interfaces

1 From the WebPublisher Application object's Templates page, click Define User Interfaces to display the Define User Interfaces dialog box.



Each user interface is generated from the assigned templates and content type.

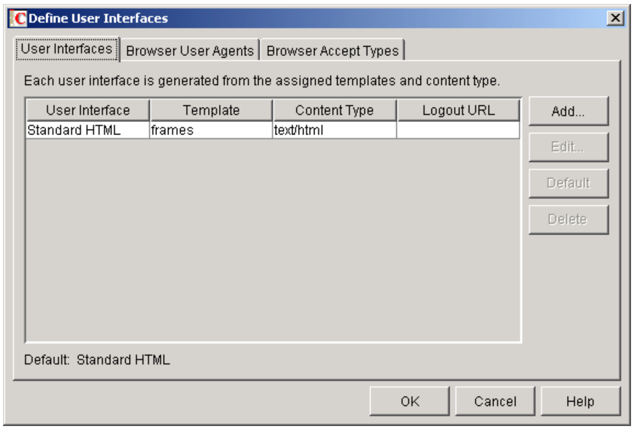
User Interface	Template	Content Type	Logout URL
Standard HTML	frames	text/html	

Default: Standard HTML

The dialog box includes three tabs:

- **User Interfaces:** The User Interfaces tab lets you add, modify, and remove user interfaces, as well as determine whether or not GroupWise data added to an interface should be cached on proxy servers. Each interface consists of template files that support a specific content type. For example, the predefined Standard HTML interface uses frame-based HTML templates, located in the frames directory, that support the text/html content type.
- **Browser User Agents:** The Browser User Agents tab lets you associate a user interface with a Web browser. The association is based on the browser's User Agent information (signature, platform, version, and so forth).
- **Browser Accept Types:** The Browser Accept Types tab lets you associate a user interface with a Web browser. The association is based on the content type the browser will accept.

2 To add, remove, or modify user interfaces, click the User Interfaces tab.



Each user interface is generated from the assigned templates and content type.

User Interface	Template	Content Type	Logout URL
Standard HTML	frames	text/html	

Default: Standard HTML

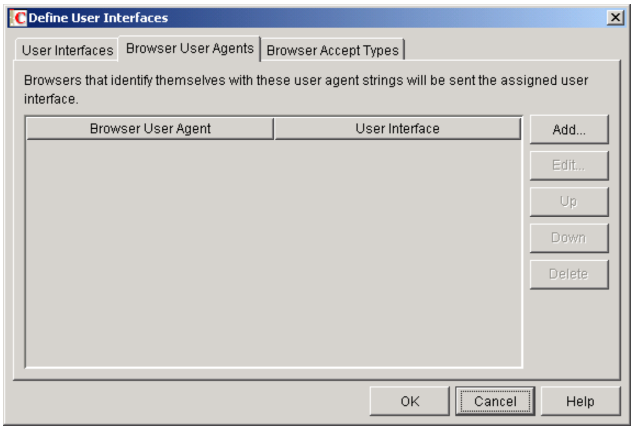
The User Interface list displays all available user interfaces. The list includes the following information:

- **User Interface:** This column displays the name assigned to the user interface (for example, Standard HTML).
- **Template:** This column displays the directory in which the template files are located. Only the directory name is shown. You can append this directory name to the template path shown on the Templates page to see the full template directory path.
- **Content Type:** This column displays the content type required by the templates (for example, text/html, text/x-hdml, or text/vnd.wap.wml).
- **Logout URL:** By default, when a user logs out, he or she is returned to the standard login page. When adding or editing the user interface, you can use the logout URL to define a different page. If you do so, this column displays the URL. This URL overrides the logout URL specified on the WebPublisher Application object's Environment page (see "Modifying the Speller Application Environment Settings" on page 854).

Choose from the following options to manage the user interfaces:

- **Add:** Click Add to add a user interface to the list.
- **Edit:** Select a user interface in the list, then click Edit to edit the interface's name, template directory, content type, or proxy caching setting.
- **Default:** Select a user interface in the list, then click Default to make that interface the default interface. The WebPublisher Application will use the default interface only if it can't determine the appropriate interface based on the browser's User Agent (Browser User Agent tab) or the browser's accepted content types (Browser Accept Types tab).
- **Delete:** Select a user interface in the list, then click Delete to remove the interface. This only removes the entry from the list. It does not delete the template files from the template directory.

3 To associate a user interface with a Web browser based on the browser's User Agent information, click the Browser User Agents tab.



Browsers that identify themselves with these user agent strings will be sent the assigned user interface.

Browser User Agent	User Interface

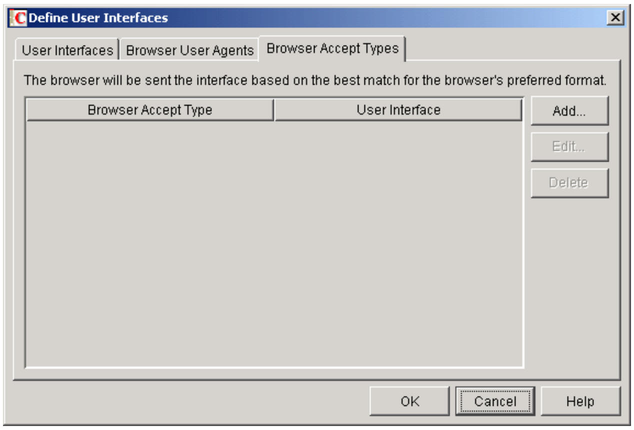
The Browser User Agents tab lets you associate a user interface with a Web browser. The association is based on the browser's User Agent information (signature, platform, version, and so forth). For example, if a browser's User Agent information includes "Windows CE" and you've created a specialized Windows CE user interface (templates), you could associate the User Agent and user interface so that Windows CE users would see your specialized Windows CE user interface.

If a browser's User Agent information matches more than one entry in the list, the application uses the first entry. If the browser's User Agent information does not match any entries in the list, the WebPublisher Application tries to select an interface based on the content types the browser will accept (Browser Accept Types tab). If no match is made based on the Accept Types information, the WebPublisher Application uses the default user interface listed on the User Interfaces tab.

Choose from the following options to manage the associations:

- **Add:** Click Add to add an entry to the list.
- **Edit:** Select an entry from the list, then click Edit to edit the entry's information.
- **Up:** Select an entry from the list, then click Up to move it up in the list. If two entries match the information in a browser's User Agent header, the WebPublisher Application uses the interface associated with the first entry listed.
- **Down:** Select an entry from the list, then click Down to move it down in the list.
- **Delete:** Select an entry from the list, then click Delete to remove the entry.

4 To associate a user interface with a Web browser based on the content type that the browser will accept, click the Browser Accept Types tab.



The browser will be sent the interface based on the best match for the browser's preferred format.

Browser Accept Type	User Interface

The Browser Accept Types tab lets you associate a user interface with a Web browser. The association is based on the content type the browser will accept.

Many browsers accept more than one content type (for example, both text/html and text/plain). If the list contains more than one acceptable content type, the WebPublisher Application uses the browser's preferred content type, which is the type that is listed first in the browser's Accept Type header.

If no interface can be determined based on the entries in the list, the WebPublisher Application uses the default user interface listed on the User Interfaces tab.

Choose from the following options to manage the associations:

- **Add:** Click Add to add an entry to the list.
- **Edit:** Select an entry from the list, then click Edit to edit the entry's information.
- **Delete:** Select an entry from the list, then click Delete to remove the entry.

5 Click OK to save your changes and return to the WebPublisher Application object's Templates page.

Controlling Availability of WebPublisher Features

WebPublisher users can:

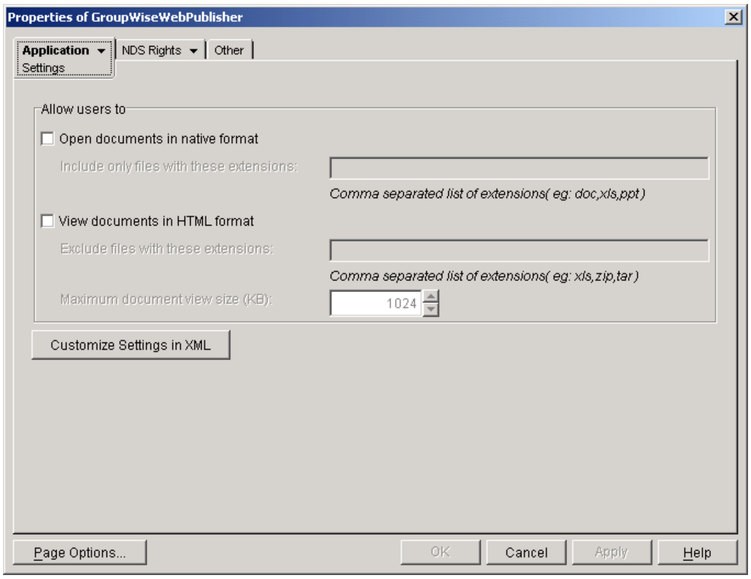
- View documents in HTML format.
- Open documents in native format.

All users who access WebPublisher through a single Web server will have the same feature access. You cannot configure individual user settings. However, if you have multiple Web servers, you can establish different settings for the Web servers by completing the following steps for each server's WebPublisher Application.

To configure the WebPublisher Application's user settings:

1 In ConsoleOne, right-click the WebAccess Application object, then click Properties.

2 Click Application > Settings to display the Settings page.



Allow users to

□ Open documents in native format

Include only files with these extensions:

Comma separated list of extensions(eg: doc,xls,ppt)

□ View documents in HTML format

Exclude files with these extensions:

Comma separated list of extensions(eg: xls,zip,tar)

Maximum document view size (KB): 1024

3 Configure the following settings:

Open Documents in Native Format: By default, the Save As option enables user to save library documents to their local drives and then open them in their native applications. You can turn on this option to enable the Open option. The Open option enables users to open documents directly in their native applications without first saving the files to the local drive.

This option requires that 1) each user's Web browser knows the correct application or plug-in to associate with the document, according to its file extension or MIME type, and 2) the application or plug-in is available to the user. Otherwise, the user will be prompted to save the file to disk or specify the application to open it.

This option and the View Documents in Native Format option can both be enabled at the same time. Doing so gives users both the Open option and the View option, which means they have the choice of opening a document in its native application or viewing it as HTML.

- **Include Only Files With These Extensions:** If you want only certain file types to be have the Open option, enter the file types in the Include Only Files With These Extensions field. Include only the extension and separate each extension with a comma (for example, doc, xls, ppt). The Open option will not be available for any file types not entered in this field.

View Documents in HTML Format: Enable this option if you want users to be able to view library documents in HTML format. Disable this option to require users to save a document to a local drive and view it in its native application. WebAccess uses Stellent Outside In HTML Export to convert files to HTML format.

For a list of the supported file format conversions, download the following document from the Stellent Web site:

OutSide In Supported Platforms and File Formats (http://www.stellent.com/stellent3/groups/mkt/documents/nativepage/outside_in_supported_platforms.pdf)

This option and the Open Documents in Native Format option can both be enabled at the same time. Doing so gives users both the View option and the Open option, which means they have the choice of viewing a document as HTML or opening it in its native application.

- **Exclude Files With These Extensions:** If you want to exclude certain file types from having the View option, enter the file types in the Exclude Files With These Extensions field. Include only the extension and separate each extension with a comma (for example, doc, xls, ppt). The View option will be available for any file types not entered in this field.

- **Maximum Document View Size:** Specify the maximum size file that can be viewed in HTML format. If a file exceeds the maximum size, it must be opened in native format (if allowed) rather than viewed in HTML format. The default maximum size is 1024 KB.

4 Click OK.

Configuring the GroupWise Service Provider

The GroupWise® service provider is installed and configured when you install the WebAccess Application to a Web server. The GroupWise service provider receives GroupWise requests from the WebAccess Application and communicates with the WebAccess Agent to fill the requests.

The WebAccess installation program creates a Novell® eDirectory™ object for the GroupWise service provider in the same context as the WebAccess Application. The object is named GroupWiseProvider. Using ConsoleOne®, you can modify the GroupWiseProvider object to:

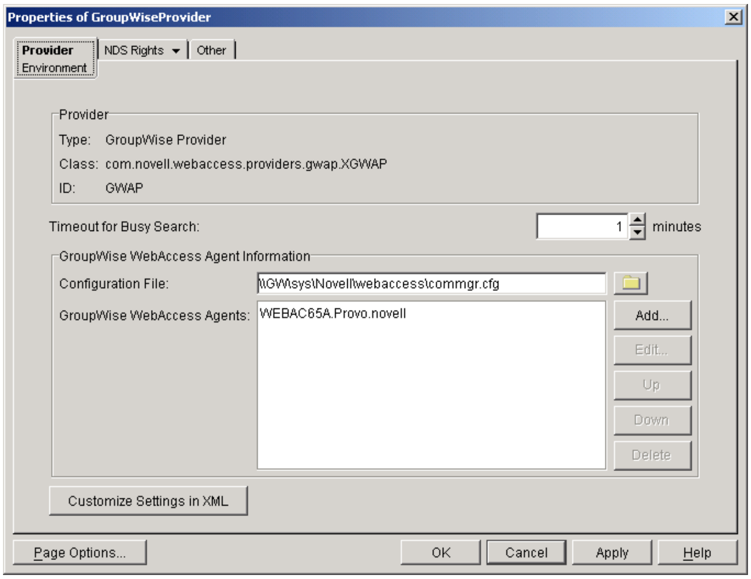
- Change how long the service provider will wait for the WebAccess Agent to return information for a Busy Search. Users can perform Busy Searches when scheduling appointments to ensure that the appointment's recipients will be available at the scheduled time. The default timeout interval is 1 minute.
- Define the WebAccess Agents that the service provider will contact to fill GroupWise requests. If your GroupWise system includes more than one WebAccess Agent, you can use this feature to provide failover support.

To modify the GroupWise service provider's configuration:

1 In ConsoleOne, right-click the GroupWise service provider object (GroupWiseProvider), then click Properties.

NOTE: The GroupWise service provider object is not available in the GroupWise View. To locate the GroupWise service provider object, you must use the Console View.

2 If necessary, click Provider > Environment to display the Environment page.



Properties of GroupWiseProvider

Provider

Type: GroupWise Provider

Class: com.novell.webaccess.providers.gwap.XGWAP

ID: GWAP

Timeout for Busy Search: 1 minutes

GroupWise WebAccess Agent Information

Configuration File: \\GW\sys\Novell\webaccess\commgr.cfg

GroupWise WebAccess Agents: WEBAC65A.Provo.novell

3 Choose from the following options:

Timeout for Busy Search: Select how long you want the GroupWise service provider to wait for the WebAccess Agent to return information when a user performs a Busy Search.

Configuration File: The WebAccess Agent's configuration file (commgr.cfg) contains the agent's IP address and the encryption key required by the GroupWise service provider to communicate with the WebAccess Agent. By default, the commgr.cfg file is stored in the WebAccess Application's home directory (novell\webaccess on the Web server or /opt/novell/groupwise/webaccess on Linux).

In general, you should not need to change this setting. However, if you have multiple WebAccess Agents in your GroupWise system and you are optimizing WebAccess to provide greater scalability and availability, you might need to change the setting. For information, see "Configuring Redirection and Failover Support" on page 810.

GroupWise WebAccess Agents: This list displays the WebAccess Agents the GroupWise service provider can communicate with when attempting to complete a request. If the first one listed is unavailable, the GroupWise service provider will attempt to use the second, third, fourth, and so on until it is successful. This provides failover support and ensures greater availability for your WebAccess users. For more information about optimizing availability, see "Configuring Redirection and Failover Support" on page 810.

The list must include at least one WebAccess Agent.

To add a WebAccess Agent to the list, click Add to browse for and select the WebAccess Agent object, then click OK.

To edit a WebAccess Agent's information, select the WebAccess Agent in the list, then click Edit.

To remove a WebAccess Agent from the list, select the WebAccess Agent in the list, then click Delete.

Customize Settings in XML: Click this button to launch the XML editor. You can use the editor to add, modify, or delete GroupWise service provider settings.

4 Click OK to save the changes.

Configuring the LDAP Service Provider

The LDAP service provider is installed and configured when you install the WebAccess Application to a Web server. The LDAP service provider receives LDAP directory requests from the WebAccess Application and communicates with LDAP services to fill the requests.

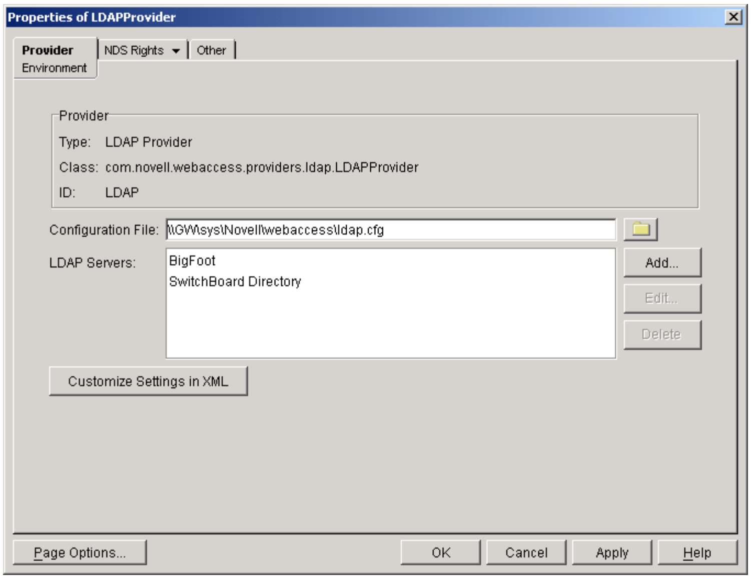
The GroupWise® WebAccess installation program creates a Novell® eDirectory™ object for the LDAP service provider in the same context as the WebAccess Application. The object is named LDAPProvider. Using ConsoleOne®, you can modify the LDAPProvider object to define the LDAP services that the service provider can contact.

To modify the LDAP service provider's configuration:

1 In ConsoleOne, right-click the LDAP service provider object (LDAPProvider), then click Properties.

NOTE: The LDAP service provider object is not available in the GroupWise View. To locate the LDAP service provider object, you must use the Console View.

2 If necessary, click Provider > Environment to display the Environment page.



Provider

Type: LDAP Provider

Class: com.novell.webaccess.providers.ldap.LDAPProvider

ID: LDAP

Configuration File: \\GW\sys\Novell\webaccess\ldap.cfg

LDAP Servers: BigFoot
SwitchBoard Directory

3 Choose from the following options:

Configuration File: The LDAP service provider's configuration file (ldap.cfg) contains the information for the LDAP services defined in the LDAP servers list. Because the LDAP service provider cannot access eDirectory or the GroupWise databases for this information, ConsoleOne writes the information to the ldap.cfg file.

By default, the ldap.cfg file is stored in the WebAccess Application's home directory (novell\webaccess on the Web server or /opt/novell/groupwise/webaccess on Linux). You should avoid changing the location of the file. If you do change the location of the file, you need to make sure to modify the ldap.cfg path in the Java servlet engine's properties file. If you do not, the LDAP service provider will continue to look for its configuration information in the old location.

LDAP Servers: This list displays the LDAP services the LDAP service provider can communicate with. The GroupWise WebAccess Address Book will list all LDAP services shown in the list.

To add an LDAP service to the list, click Add to display the Add LDAP Server dialog box, fill in the required information, then click OK. For information about each of the fields, click Help in the Add LDAP Server dialog box.

To edit an LDAP service's information, select the LDAP service in the list, then click Edit.

To remove an LDAP service from the list, select the LDAP service in the list, then click Delete.

Customize Settings in XML: Click this button to launch the XML editor. You can use the editor to add, modify, or delete LDAP service provider settings.

4 Click OK to save the changes.

Configuring the GroupWise Document Service Provider

The GroupWise® Document service provider is installed and configured when you install the WebPublisher Application to a Web server. The GroupWise Document service provider receives GroupWise document requests from the WebPublisher Application and communicates with the WebAccess Agent to fill the requests.

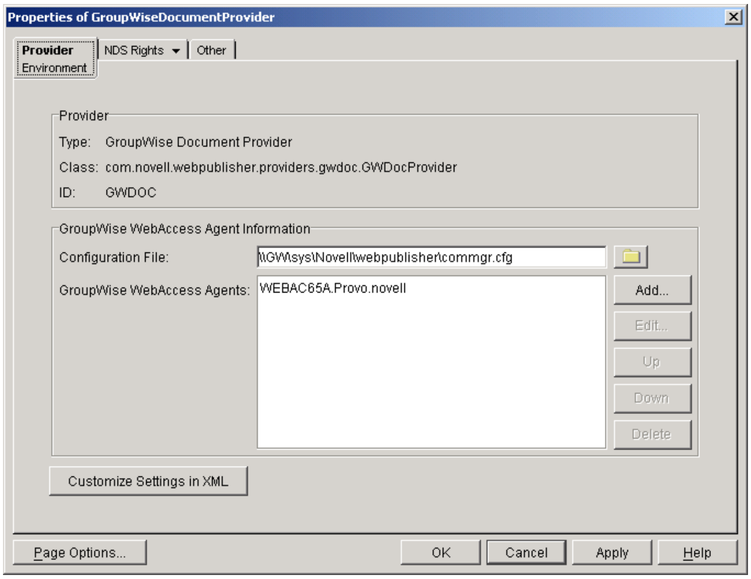
The WebAccess installation program creates a Novell® eDirectory™ object for the GroupWise Document service provider in the same context as the WebPublisher Application. The object is named GroupWiseDocumentProvider. Using ConsoleOne®, you can modify the GroupWiseDocumentProvider object to define the WebAccess Agents that the service provider will contact to fill GroupWise document requests. If your GroupWise system includes more than one WebAccess Agent, you can use this feature to provide failover support.

To modify the GroupWise Document service provider's configuration:

1 In ConsoleOne, right-click the GroupWise Document service provider object (GroupWiseDocumentProvider), then click Properties.

NOTE: The GroupWise Document service provider object is not available in the GroupWise View. To locate the GroupWise Document service provider object, you must use the Console View.

2 If necessary, click Provider > Environment to display the Environment page.



Properties of GroupWiseDocumentProvider

Provider

Type: GroupWise Document Provider

Class: com.novell.webpublisher.providers.gwdoc.GWDocProvider

ID: GWDOC

GroupWise WebAccess Agent Information

Configuration File: \\GW\sys\Novell\webpublisher\commgr.cfg

GroupWise WebAccess Agents: WEBAC65A.Provo.novell

3 Choose from the following options:

Configuration File: The WebAccess Agent's configuration file (commgr.cfg) contains the agent's IP address and the encryption key required by the GroupWise Document service provider to communicate with the WebAccess Agent. By default, the commgr.cfg file is stored in the WebPublisher Application's home directory (novell\webpublisher on the Web server or /opt/novell/groupwise/webpublisher on Linux).

In general, you should not need to change this setting. However, if you have multiple WebAccess Agents in your GroupWise system and you are optimizing WebPublisher to provide greater scalability and availability, you might need to change the setting. For information, see "Configuring Redirection and Failover Support" on page 810.

GroupWise WebAccess Agents: This list displays the WebAccess Agents the GroupWise Document service provider can communicate with when attempting to complete a request. If the first one listed is unavailable, the GroupWise Document service provider will attempt to use the second, third, fourth, and so on until it is successful. This provides failover support and ensures greater availability for your WebPublisher users. For more information about optimizing availability, see "Configuring Redirection and Failover Support" on page 810.

The list must include at least one WebAccess Agent.

To add a WebAccess Agent to the list, click Add to browse for and select the WebAccess Agent object, then click OK.

To edit a WebAccess Agent's information, select the WebAccess Agent in the list, then click Edit.

To remove a WebAccess Agent from the list, select the WebAccess Agent in the list, then click Delete.

Customize Settings in XML: Click this button to launch the XML editor. You can use the editor to add, modify, or delete GroupWise Document service provider settings.

4 Click OK to save the changes.

60 Customizing the WebAccess Interface

GroupWise® WebAccess enables you to change the default Novell® logo and colors used in the WebAccess interface. For example, you can add your company logo to the main WebAccess window and change the colors to match your company colors.

You use the customization.properties file to change the logo and colors.

1 Open the customization.properties file with a text editor.

The file is located in the following directory:

NetWare and Windows: *tomcat_dir*\webapps\ROOT\WEB-INF\classes\com\novell\webaccess\templates
Linux: *tomcat_dir*/webapps/gw/WEB-INF/classes/com/novell/webaccess/templates

2 If you want to change the logo image:

2a Locate the CUSTOMIZABLE IMAGE FOR GROUPWISE WEBACCESS section at the beginning of the file.

2b To turn on customization for the logo image, set the WebAccess.Customize.Image.enable property to TRUE:

```
WebAccess.Customize.Image.enable=true
```

2c Modify the image properties as desired. The customization.properties file contains descriptions of each property.

3 If you want to change the WebAccess colors:

3a Locate the CUSTOMIZABLE COLORS SCHEME FOR GROUPWISE WEBACCESS section in the file.

3b To turn on customization of the colors, set the WebAccess.Customize.Color.enable setting to TRUE:

```
WebAccess.Customize.Color.enable=true
```

3c Modify the color properties as desired. The customization.properties file contains descriptions of each property.

4 Save the customization.properties file.

5 Restart the Web server.

6 In a Web browser, clear the browser cache, then log in to GroupWise WebAccess.

61 Monitoring WebAccess Operations

The WebAccess Agent can be monitored at the server where it runs and also in your Web browser. The WebAccess Application can be monitored in your Web browser.

- "Monitoring the WebAccess Agent" on page 875
- "Monitoring the WebAccess Application" on page 882

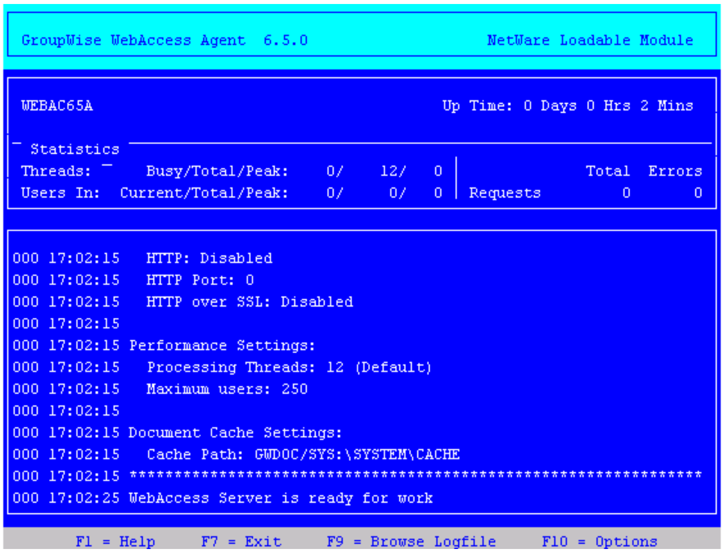
Monitoring the WebAccess Agent

The following sections explain the various methods you can use to monitor the GroupWise® WebAccess Agent to ensure that it is operating properly.

- "Monitoring the NetWare WebAccess Agent" on page 875
- "Monitoring the Windows WebAccess Agent" on page 877
- "Monitoring the Linux WebAccess Agent" on page 878
- "Monitoring the WebAccess Agent through the Web Console" on page 879
- "Monitoring the WebAccess Agent through NetWare 6.5 Remote Manager" on page 881

Monitoring the NetWare WebAccess Agent

The NetWare® WebAccess Agent console, shown below, lets you monitor the operation of the agent, view the agent's log information, and change the log settings while at the server.



```
GroupWise WebAccess Agent  6.5.0                       NetWare Loadable Module

WEBAC65A                                         Up Time: 0 Days 0 Hrs 2 Mins

 Statistics
Threads:       Busy/Total/Peak:    0/    12/    0 |                Total  Errors
Users In:  Current/Total/Peak:    0/     0/    0 | Requests           0       0

000 17:02:15   HTTP: Disabled
000 17:02:15   HTTP Port: 0
000 17:02:15   HTTP over SSL: Disabled
000 17:02:15
000 17:02:15 Performance Settings:
000 17:02:15   Processing Threads: 12 (Default)
000 17:02:15   Maximum users: 250
000 17:02:15
000 17:02:15 Document Cache Settings:
000 17:02:15   Cache Path: GWDOC/SYS:\SYSTEM\CACHE
000 17:02:15 *****************************************************************
000 17:02:25 WebAccess Server is ready for work
```

The console and its options are described below.

Up Time

The Up Time field displays how long it has been since the WebAccess Agent was started.

Threads

The default of 12 threads enables the WebAccess Agent to service 12 user requests at one time. The Busy field displays the number of threads that are currently servicing user requests. The Total field displays the total number of threads available to service requests (by default, 12). The Peak field displays the most threads used at one time to service requests. If all threads are busy much of the time, you can increase the number of threads available for use. See "Modifying WebAccess Settings" on page 829.

Users In

The Users In field displays the number of users who currently are logged in. During startup, if you have enabled WebPublisher, the WebAccess Agent logs in one time for each available thread; these logins are reflected in the Users In fields. The Total field displays the total number of users who have logged in during the current up time. The Peak field displays the most users who have been logged in at one time.

By default, a maximum of 250 users can be logged in at one time. You can use the /maxusers startup switch to change the default. See "Using WebAccess Agent Startup Switches" on page 895.

Requests

The Total field displays the total number of requests the WebAccess Agent has processed during its current up time. The Errors field lists the number of requests that could not be processed because of errors.

Logging Box

The Logging box displays the logged information. The current log level determines the amount of information that is displayed (see "F10 = Options" on page 876). For each line, the first item is the number of the thread that processed the user's request, the second item is the time of the request, and the third item is the information associated with the request.

F7 = Exit

Press F7 to shut down the WebAccess Agent.

F9 = Browse Logfile

Press F9 to view the log file. If disk logging is turned on, the current log file is displayed. If disk logging is turned off, a list of old log files is displayed (if any exist). You can then choose which log file you want to view.

F10 = Options

Press F10, then select View Log Files or Logging Options. Using the logging options, you can specify the logging level, turn disk logging on or off, specify the number of days to keep old log files, and specify the maximum amount of disk space to use for log files.

Any changes you make to the logging options apply only to the current session. When you restart the WebAccess Agent, the logging level is reset to the level specified in ConsoleOne® or in the startup file (strtweb.ncf).

Log Level: Off turns logging off; Normal displays initial statistics, user logins, warnings, and errors; Verbose displays Normal logging plus user requests; and Diagnostic displays Verbose logging plus thread information. The default is Normal logging. Use Diagnostic only if you are troubleshooting a problem with WebAccess.

File Logging: Turns disk logging on or off. When disk logging is turned on, the WebAccess Agent creates a new log file each day and each time it is restarted. The log file is named *mmdd*web.*nnn*, where *mm* is the month, *dd* is the day, and *nnn* is a sequenced number (001 for the first log file of the day, 002 for the second, and so forth). The default location for the log files is the *domain*\wpgate\webac65a\*xxx*.prc directory.

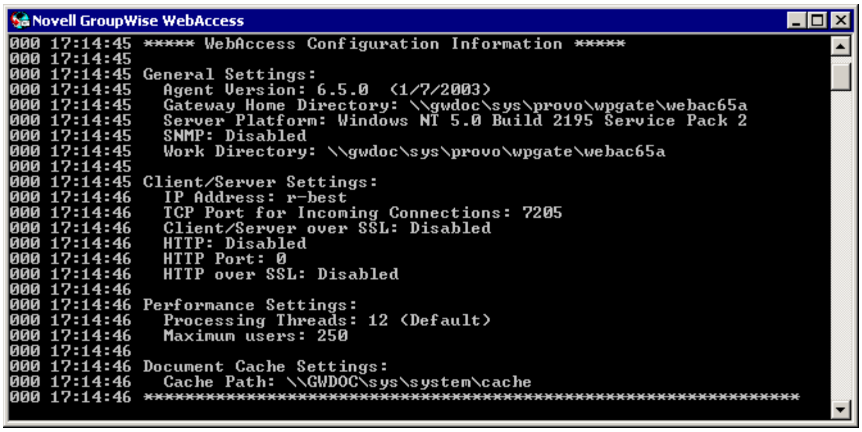
The verbose and diagnostic logging levels do not degrade WebAccess Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Max Log File Age: Specifies the number of days you want the WebAccess Agent to retain old log files. The WebAccess Agent will retain the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.

Max Log Disk Space: Specifies the maximum amount of disk space you want to use for log files. If the disk space limit is exceeded, the WebAccess Agent will delete log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 65536 KB.

Monitoring the Windows WebAccess Agent

The Windows WebAccess Agent console lets you monitor the operation of the agent. The console, shown below, is displayed in a DOS window.



```
000 17:14:45 ***** WebAccess Configuration Information *****
000 17:14:45
000 17:14:45 General Settings:
000 17:14:45   Agent Version: 6.5.0  (1/7/2003)
000 17:14:45   Gateway Home Directory: \\gwdoc\sys\provo\wpgate\webac65a
000 17:14:45   Server Platform: Windows NT 5.0 Build 2195 Service Pack 2
000 17:14:45   SNMP: Disabled
000 17:14:45   Work Directory: \\gwdoc\sys\provo\wpgate\webac65a
000 17:14:45
000 17:14:45 Client/Server Settings:
000 17:14:46   IP Address: r-best
000 17:14:46   TCP Port for Incoming Connections: 7205
000 17:14:46   Client/Server over SSL: Disabled
000 17:14:46   HTTP: Disabled
000 17:14:46   HTTP Port: 0
000 17:14:46   HTTP over SSL: Disabled
000 17:14:46
000 17:14:46 Performance Settings:
000 17:14:46   Processing Threads: 12 (Default)
000 17:14:46   Maximum users: 250
000 17:14:46
000 17:14:46 Document Cache Settings:
000 17:14:46   Cache Path: \\GWDOC\sys\system\cache
000 17:14:46 ****************************************************************
```

The console and its options are described below.

Logging Window

The current logging level determines the amount of information that is displayed. You can specify the logging level through ConsoleOne, through startup switches, or by using the F2 function key. See "Modifying Log Settings in ConsoleOne" on page 833, "Modifying Log Settings through Startup Switches" on page 834, and "F2" on page 878.

The verbose and diagnostic logging levels do not degrade WebAccess Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

For each line, the first item is the number of the thread that processed the user's request, the second item is the time of the request, and the third item is the information associated with the request.

F1 or F7

Shuts down and exits the agent.

F2

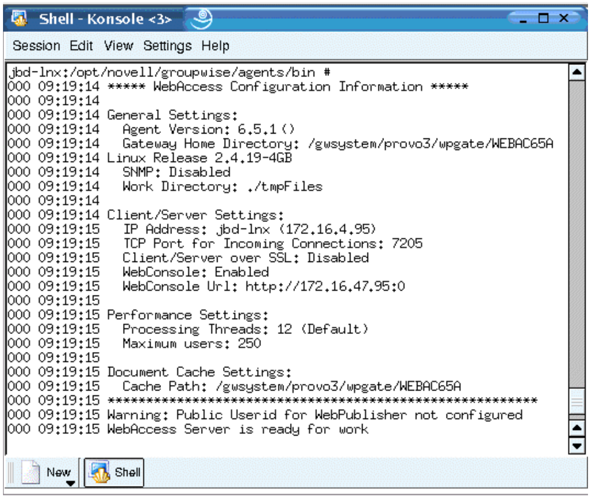
Cycles the logging level between Normal, Verbose, and Diagnostic. Normal displays initial statistics, user logins, warnings, and errors; Verbose displays Normal logging plus user requests; and Diagnostic displays Verbose logging plus thread information. The default is Normal logging. Use Verbose only if you are troubleshooting a problem with WebAccess.

The verbose and diagnostic logging levels do not degrade WebAccess Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Any changes you make to the logging level using F2 apply only to the current session. When you restart the WebAccess Agent, the logging level is reset to the level specified in ConsoleOne or in the startup file (strtweb.bat).

Monitoring the Linux WebAccess Agent

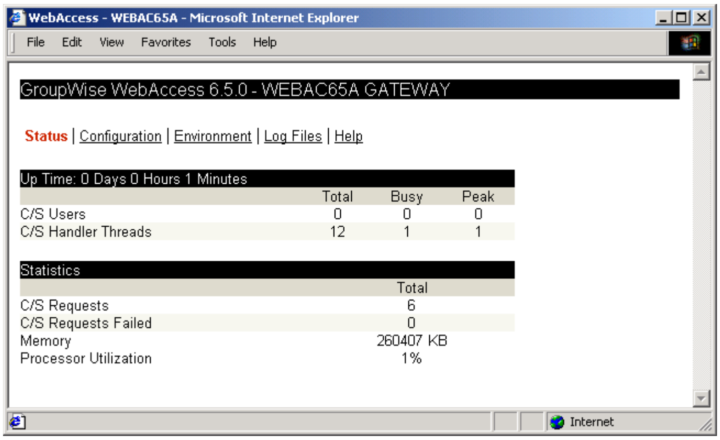
By default, the Linux Agent runs as a daemon with no user interface. To display information on the server where the WebAccess Agent runs, you must start the WebAccess Agent with the --show startup switch. The console is displayed in a terminal window.



```
jbd-lnx:/opt/novell/groupwise/agents/bin #
000 09:19:14 ***** WebAccess Configuration Information *****
000 09:19:14
000 09:19:14 General Settings:
000 09:19:14   Agent Version: 6.5.1 ()
000 09:19:14   Gateway Home Directory: /gwsystem/provo3/wpgate/WEBAC65A
000 09:19:14 Linux Release 2.4.19-4GB
000 09:19:14   SNMP: Disabled
000 09:19:14   Work Directory: ./tmpFiles
000 09:19:14
000 09:19:14 Client/Server Settings:
000 09:19:15   IP Address: jbd-lnx (172.16.4.95)
000 09:19:15   TCP Port for Incoming Connections: 7205
000 09:19:15   Client/Server over SSL: Disabled
000 09:19:15   WebConsole: Enabled
000 09:19:15   WebConsole Url: http://172.16.47.95:0
000 09:19:15
000 09:19:15 Performance Settings:
000 09:19:15   Processing Threads: 12 (Default)
000 09:19:15   Maximum users: 250
000 09:19:15
000 09:19:15 Document Cache Settings:
000 09:19:15   Cache Path: /gwsystem/provo3/wpgate/WEBAC65A
000 09:19:15 ********************************************************
000 09:19:15 Warning: Public Userid for WebPublisher not configured
000 09:19:15 WebAccess Server is ready for work
```

Monitoring the WebAccess Agent through the Web Console

You can use a Web browser interface, referred to as the Web console, to monitor the WebAccess Agent.


WebAccess - WEBAC65A - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Internet

GroupWise WebAccess 6.5.0 - WEBAC65A GATEWAY

Status | Configuration | Environment | Log Files | Help

Up Time: 0 Days 0 Hours 1 Minutes

	Total	Busy	Peak
C/S Users	0	0	0
C/S Handler Threads	12	1	1

Statistics

	Total
C/S Requests	6
C/S Requests Failed	0
Memory	260407 KB
Processor Utilization	1%

Through the Web console you can view the following information:

- **Status:** Displays how long the WebAccess Agent has been up; the number of client/server users who have logged in, the number of threads dedicated to handling requests, and the number of successful and failed requests; and the amount of memory on the server and the percent of processor utilization.
- **Configuration:** Displays the gateway home directory being used by the WebAccess Agent, the current log settings, the performance settings (processing threads and maximum users), and the client/server settings (IP address, TCP port, and so forth).
- **Environment:** Displays server information such as name, operating system date, memory, processor utilization, and loaded modules.
- **Log Files:** Lets you view the contents of the WebAccess Agent's log files and the current log settings.

For detailed information about each field on the Status, Configuration, Environment, or Log Files page, select the page, then click Help.

You cannot use the Web console to change any of the WebAccess Agent's settings. Changes must be made through ConsoleOne, the WebAccess Agent console, or the startup file.

Refer to the following sections for information about enabling and using the Web console:

- "Enabling the WebAccess Agent Web Console" on page 879
- "Using the WebAccess Agent Web Console" on page 881

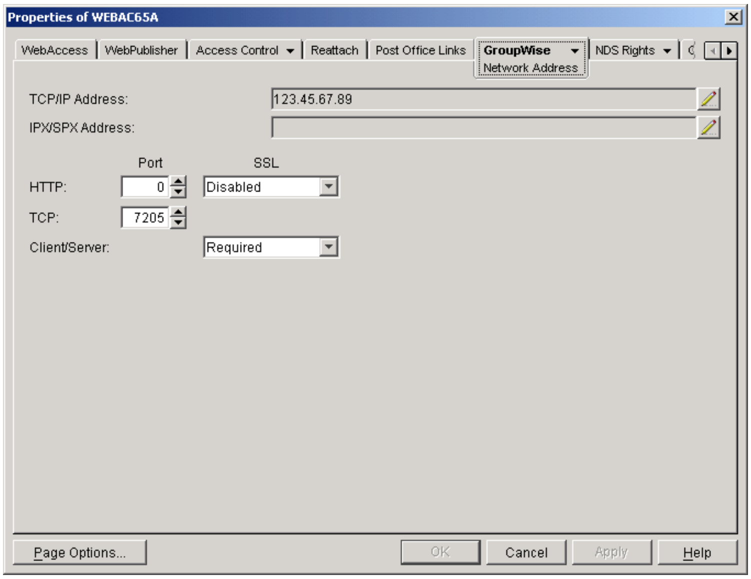
Enabling the WebAccess Agent Web Console

If, during, installation, you enabled the Web console, skip to Using the WebAccess Agent Web Console. On Linux, the Web Console is enabled by default. Skip to Using the WebAccess Agent Web Console.

If you want to enable the Web console, you need to complete the following steps.

1 In ConsoleOne, right-click the WebAccess Agent object, then click Properties.

2 Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 123.45.67.89

IPX/SPX Address:

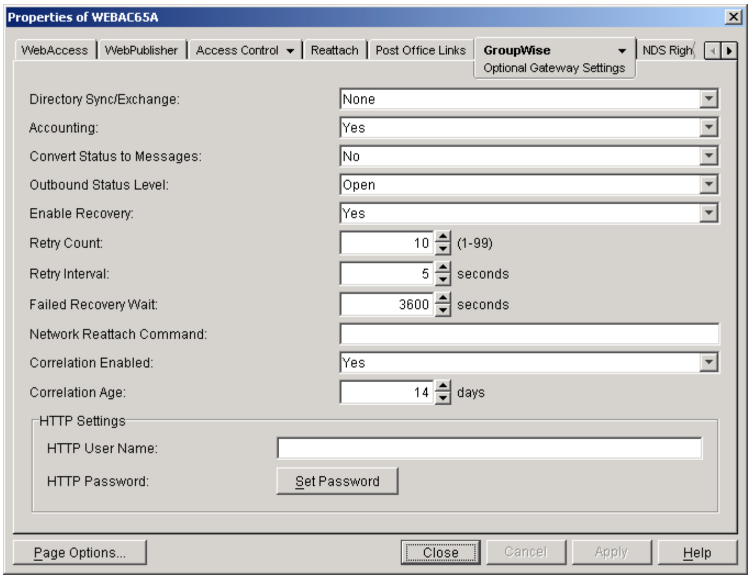
	Port	SSL
HTTP:	0	Disabled
TCP:	7205	
Client/Server:		Required

3 In the HTTP Port field, enter a port number. We recommend that you use port 7211 if it is not already in use on the WebAccess Agent's server.

Assigning a port number enables the Web console; assigning 0 as the port number disables the Web console.

Any user who knows the WebAccess Agent's IP address (or hostname) and the HTTP port number will be able to use the Web console. If you want to restrict Web console access, you can assign a username and password. To do so:

4 Click the GroupWise tab, then click Optional Gateway Settings to display the Optional Gateway Settings page.



Directory Sync/Exchange: None

Accounting: Yes

Convert Status to Messages: No

Outbound Status Level: Open

Enable Recovery: Yes

Retry Count: 10 (1-99)

Retry Interval: 5 seconds

Failed Recovery Wait: 3600 seconds

Network Reattach Command:

Correlation Enabled: Yes

Correlation Age: 14 days

HTTP Settings

HTTP User Name:

HTTP Password:

5 In the HTTP User Name field, enter an arbitrary username (for example, webcon).

6 Click Set Password to assign a password (for example, monitor).

7 Click OK to save your changes.

The Web console can only be enabled or disabled through the Network Address page (see Step 2 above). However, you can use the /httpuser and /httppassword startup switches to override the assigned username and password. For more information, see Appendix 64, “Using WebAccess Agent Startup Switches,” on page 895.

Using the WebAccess Agent Web Console

1 In a Web browser, enter the following:

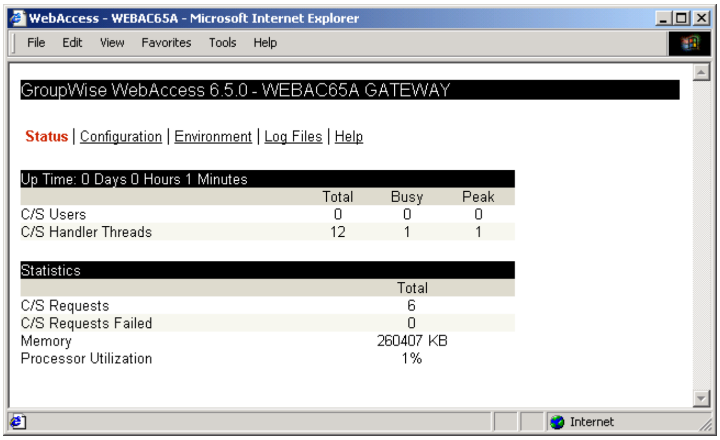
`http://`*`IP_address:agent_port`*

or

`https://`*`IP_address:agent_port`*

where *IP_address* is the IP address of the server where the WebAccess Agent is running, and *agent_port* is the port number assigned to the agent. If you used the default port during installation, the port number is 7211.

2 If prompted, enter the Web console username and password.



GroupWise WebAccess 6.5.0 - WEBAC65A GATEWAY

Status | Configuration | Environment | Log Files | Help

Up Time: 0 Days 0 Hours 1 Minutes	Total	Busy	Peak
C/S Users	0	0	0
C/S Handler Threads	12	1	1

Statistics	Total
C/S Requests	6
C/S Requests Failed	0
Memory	260407 KB
Processor Utilization	1%

3 Select Status, Configuration, Environment, or Log Files to view the desired information.

For detailed information about each field on the Status, Configuration, Environment, or Log Files page, select the page, then click Help.

Monitoring the WebAccess Agent through NetWare 6.5 Remote Manager

If the WebAccess Agent is running on a NetWare 6.5 server, you can use the IP Address Management feature in NetWare Remote Manager (NetWare Remote Manager > Manage Server > IP Address Management) to view the IP address and port configuration for the WebAccess Agent. This is also true for other GroupWise agents (MTA, POA, and Internet Agent) running on NetWare 6.5 servers.

IMPORTANT: If the WebAccess Agent is running in protected mode, it will not display in NetWare Remote Manager.

You access NetWare Remote Manager by entering the following URL in a Web browser:

`http://`*`server_address`*`:8008`

For example:

```
http://137.65.123.11:8008
```

For more information about using NetWare Remote Manager, see the NetWare 6.5 documentation (http://www.novell.com/documentation/nw65).

Monitoring the WebAccess Application

The WebAccess Application includes a Web console, similar to the WebAccess Agent's Web console, that you can use to monitor it. The Web console lets you see information about logged in users, such as their IP address, their GroupWise and Web browser versions, and the WebAccess Agent providing mailbox access. In addition, you can view the WebAccess Application's log files and configuration files, and view Java information such as the version and classpath settings.

The following sections provide information to help you use the Web console:

- "Enabling the WebAccess Application Web Console" on page 882
- "Using the WebAccess Application Web Console" on page 882
- "Understanding the WebAccess Application Web Console Information" on page 883

Enabling the WebAccess Application Web Console

1 Open the webacc.cfg file, located in the WebAccess Application's home directory (novell\webaccess on the Web server or /opt/novell/groupwise/webaccess on Linux).

2 Locate the following lines in the file:

```
Admin.WebConsole.enable=false
Admin.WebConsole.username=admin
Admin.WebConsole.password=admin
```

3 Enable the Web console by changing the FALSE entry to TRUE:

```
Admin.WebConsole.enable=true
```

4 If desired, change the default username and password. A username and password is required.

5 Save the file.

6 Restart the Java servlet engine.

Using the WebAccess Application Web Console

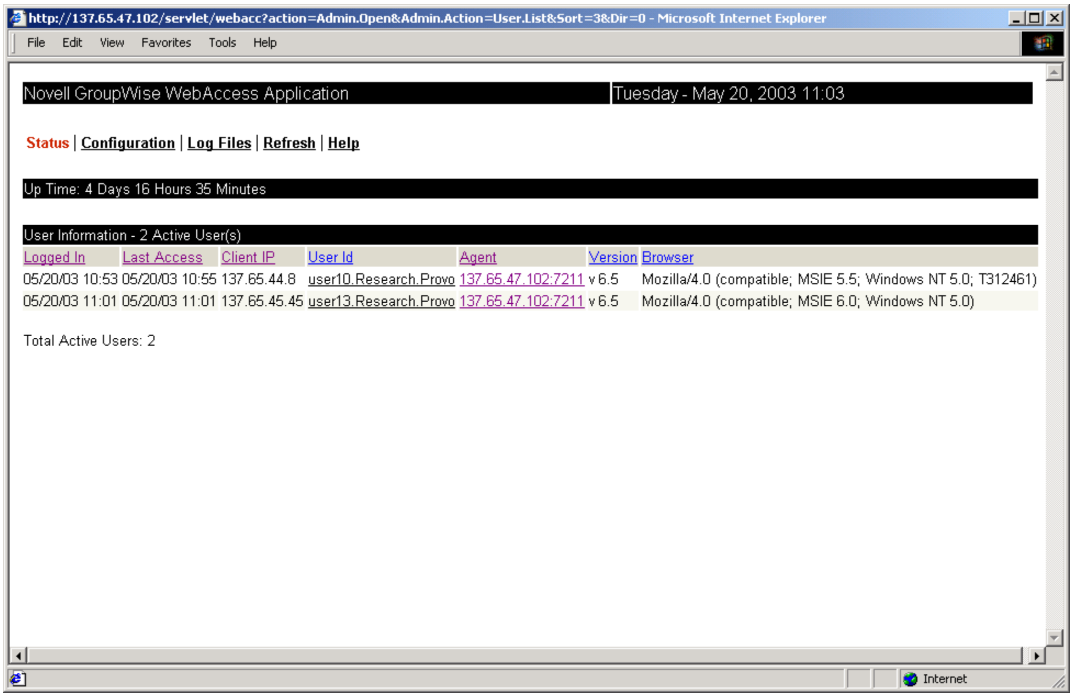
1 In a Web browser, enter the following URL:

NetWare or Windows: http://*server_address*/servlet/webacc?action=Admin.Open
Linux: http://*server_address*/gw/webacc?action=Admin.Open

where *server_address* is the Web server's IP address or DNS hostname.

2 When prompted, enter the username and password.

The Web console is displayed.


http://137.65.47.102/servlet/webacc?action=Admin.Open&Admin.Action=User.List&Sort=3&Dir=0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Internet

Novell GroupWise WebAccess Application | Tuesday - May 20, 2003 11:03

Status | Configuration | Log Files | Refresh | Help

Up Time: 4 Days 16 Hours 35 Minutes

User Information - 2 Active User(s)

Logged In	Last Access	Client IP	User Id	Agent	Version	Browser
05/20/03 10:53	05/20/03 10:55	137.65.44.8	user10.Research.Provo	137.65.47.102:7211	v 6.5	Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; T312461)
05/20/03 11:01	05/20/03 11:01	137.65.45.45	user13.Research.Provo	137.65.47.102:7211	v 6.5	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)

Total Active Users: 2

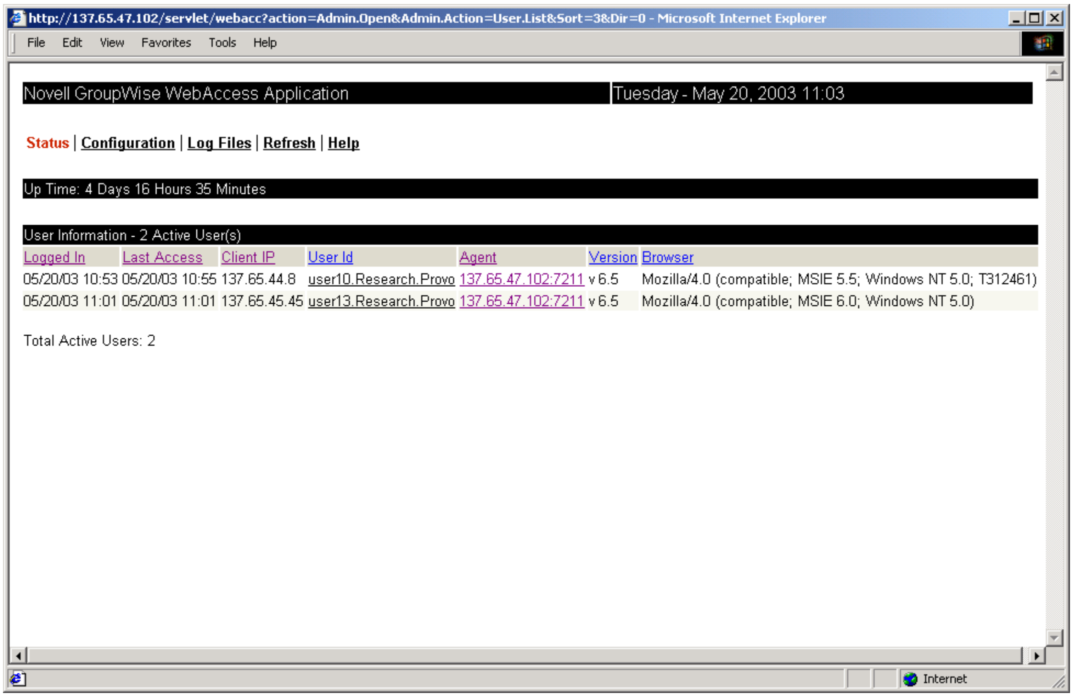
Understanding the WebAccess Application Web Console Information

The Web console information is organized into three main pages:

- "Status" on page 883
- "Configuration" on page 885
- "Log Files" on page 887

Status

The Status page, shown below, is the initial page that is displayed when you log in to the Web console. It provides information about the users who are currently logged in to GroupWise WebAccess.


http://137.65.47.102/servlet/webacc?action=Admin.Open&Admin.Action=User.List&Sort=3&Dir=0 - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Internet

Novell GroupWise WebAccess Application | Tuesday - May 20, 2003 11:03

Status | Configuration | Log Files | Refresh | Help

Up Time: 4 Days 16 Hours 35 Minutes

User Information - 2 Active User(s)

Logged In	Last Access	Client IP	User Id	Agent	Version	Browser
05/20/03 10:53	05/20/03 10:55	137.65.44.8	user10.Research.Provo	137.65.47.102:7211	v 6.5	Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; T312461)
05/20/03 11:01	05/20/03 11:01	137.65.45.45	user13.Research.Provo	137.65.47.102:7211	v 6.5	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)

Total Active Users: 2

Refresh: Click the Refresh option to refresh the status information.

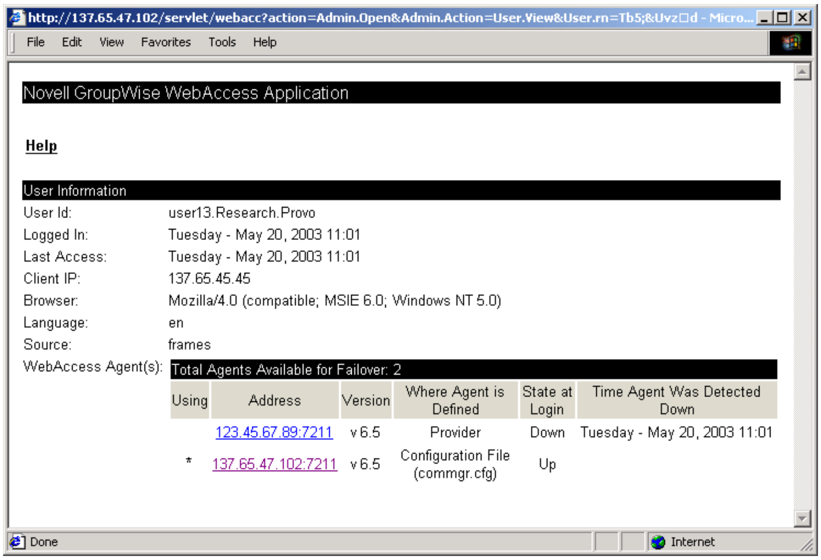
Up Time: Displays the number of days, hours, and minutes since the WebAccess Application started.

User Information: Displays information for the users currently logged in to GroupWise WebAccess. Each column is described below. Click a column heading to sort on that column.

- Logged In: Displays the date and time the user logged in.
- Last Access: Displays the date and time the user last performed a WebAccess operation that generated a request for the WebAccess Application.
- Client IP: Displays the IP address for the user's session. If you are using a proxy server, the proxy server's IP address is displayed.
- User ID: Displays the user's name, post office, and domain (userID.po.domain). You can click a user's ID to display expanded information about the user. This information is described in Expanded User Information below.
- Agent: Displays the IP address of the WebAccess Agent that is providing the user's mailbox access. You can click the agent's address to log into the agent's Web console.
- Version: Displays the version of the WebAccess Agent that is providing the user's mailbox access.
- Browser: Displays the user's Web browser version.

Expanded User Information

When you click a user's address in the User ID column, the following expanded User Information page is displayed.


http://137.65.47.102/servlet/webacc?action=Admin.Open&Admin.Action=User.View&User.rn=Tb5;&Uvz□d - Micro...
File Edit View Favorites Tools Help
Done
Internet

Novell GroupWise WebAccess Application

Help

User Information

User Id:	user13.Research.Provo
Logged In:	Tuesday - May 20, 2003 11:01
Last Access:	Tuesday - May 20, 2003 11:01
Client IP:	137.65.45.45
Browser:	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Language:	en
Source:	frames
WebAccess Agent(s):	Total Agents Available for Failover: 2

Using	Address	Version	Where Agent is Defined	State at Login	Time Agent Was Detected Down
	123.45.67.89:7211	v 6.5	Provider	Down	Tuesday - May 20, 2003 11:01
*	137.65.47.102:7211	v 6.5	Configuration File (commgr.cfg)	Up	

The User ID, Logged In, Last Access, Client IP, and Browser fields contain the same information that is displayed on the Status page. The following fields contain additional information not provided on the Status page.

Language: Displays the WebAccess language used.

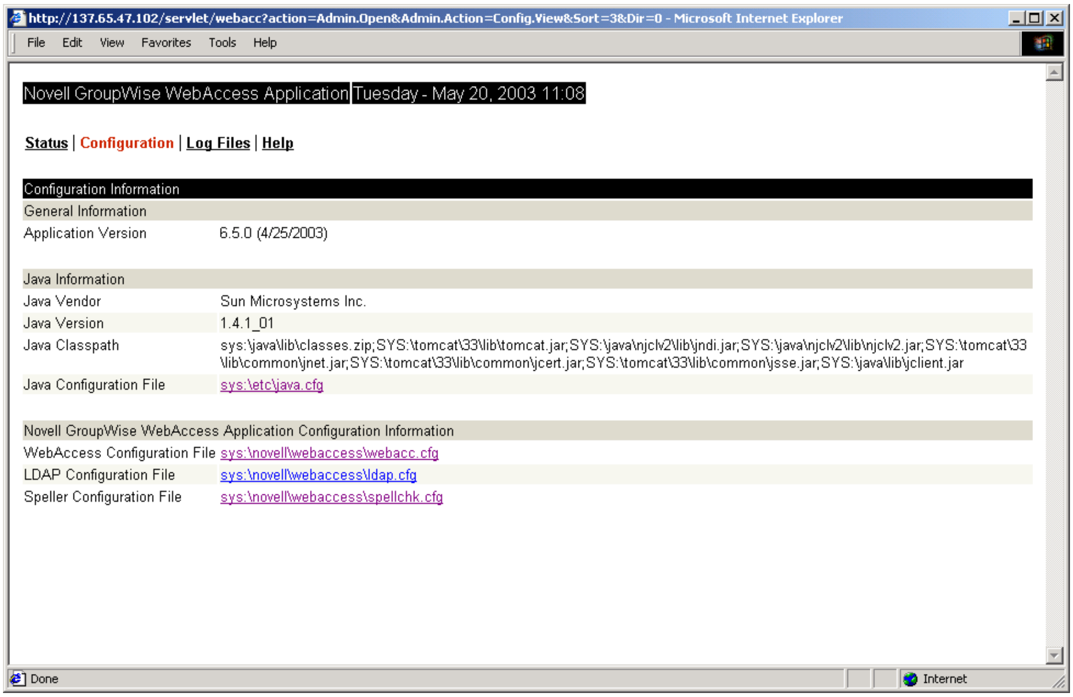
Source: Displays the WebAccess templates used.

WebAccess Agents: Displays the WebAccess Agents available to the user and each agent’s status.

- Using: An asterisk (*) indicates that the WebAccess Agent is being used to provide access to the user’s mailbox.
- Address: Displays the WebAccess Agent’s address. You can click the agent’s address to log into the agent’s Web console.
- Version: Displays the WebAccess Agent’s version.
- Where Agent Is Defined: Displays the location where the agent is defined. There are four possible locations: the user’s post office, the user’s domain, the GroupWiseWebAccess Provider, and the WebAccess commgr.cfg. For more information about where agents are defined and the order in which they are used, see “Configuring Redirection and Failover Support” on page 810.
- State at Login: Displays the state (UP or DOWN) that the WebAccess Agent was in when the user logged in to GroupWise WebAccess.
- Time Agent Was Detected Down: If the WebAccess Agent’s state is DOWN, displays the time that the DOWN state was detected.

Configuration

The Configuration page, shown below, displays the WebAccess Application’s version and Java information and lets you view the WebAccess Application configuration files.



http://137.65.47.102/servlet/webacc?action=Admin.Open&Admin.Action=Config.View&Sort=3&Dir=0 - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Done
Internet

Novell GroupWise WebAccess Application Tuesday - May 20, 2003 11:08

Status | Configuration | Log Files | Help

Configuration Information	
General Information	
Application Version	6.5.0 (4/25/2003)
Java Information	
Java Vendor	Sun Microsystems Inc.
Java Version	1.4.1_01
Java Classpath	sys:\java\lib\classes.zip;SYS:\tomcat\33\lib\tomcat.jar;SYS:\java\njclv2\lib\jndi.jar;SYS:\java\njclv2\lib\njclv2.jar;SYS:\tomcat\33\lib\common\jnet.jar;SYS:\tomcat\33\lib\common\jcert.jar;SYS:\tomcat\33\lib\common\jsse.jar;SYS:\java\lib\jclient.jar
Java Configuration File	sys:\etc\java.cfg
Novell GroupWise WebAccess Application Configuration Information	
WebAccess Configuration File	sys:\novell\webaccess\webacc.cfg
LDAP Configuration File	sys:\novell\webaccess\ldap.cfg
Speller Configuration File	sys:\novell\webaccess\spellchk.cfg

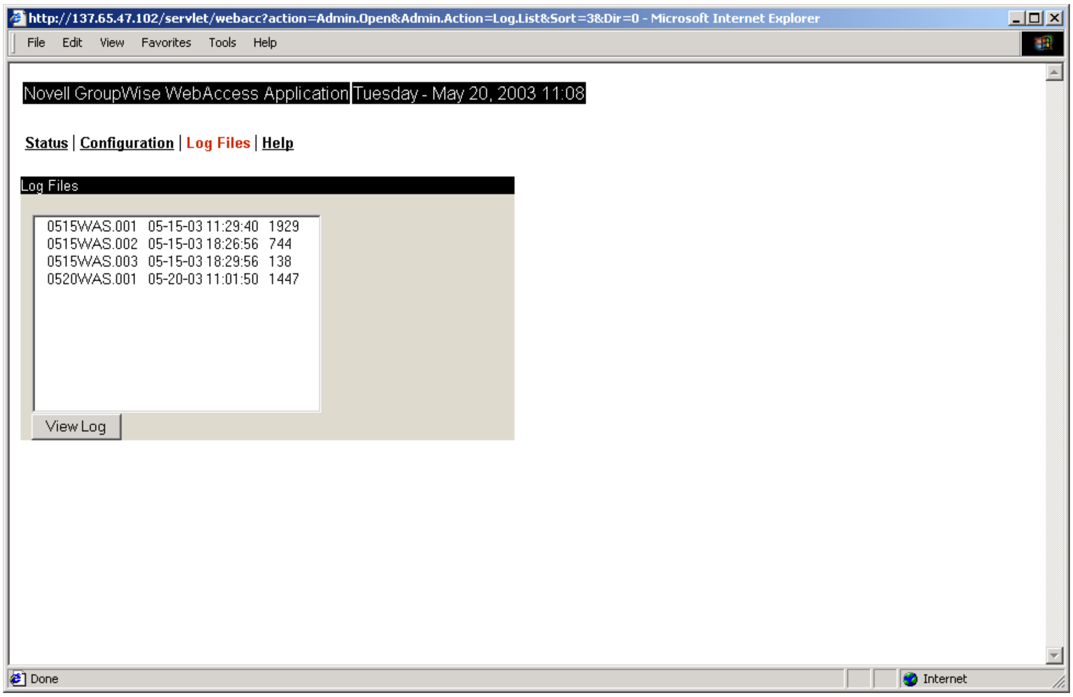
General Information: Displays the WebAccess Application's version number and date.

Java Information: Displays the Java vendor, version, and classpath information. You can click the link in the Java Configuration File field to open the configuration file for viewing. This is a view only option; you cannot make changes to the file.

Novell GroupWise WebAccess Application Configuration Information: Displays the configuration files used by the WebAccess Application. You can click the link for a file to open it for viewing. This is a view only option; you cannot make changes to the file.

Log Files

The Log Files page, shown below, lists the WebAccess Application's log files. To view a log file, select the file in the list, then click View Log.



http://137.65.47.102/servlet/webacc?action=Admin.Open&Admin.Action=Log.List&Sort=3&Dir=0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Novell GroupWise WebAccess Application Tuesday - May 20, 2003 11:08
Status | Configuration | Log Files | Help
Log Files

```
0515WAS.001  05-15-03 11:29:40  1929
0515WAS.002  05-15-03 18:26:56  744
0515WAS.003  05-15-03 18:29:56  138
0520WAS.001  05-20-03 11:01:50  1447
```

62 Securing WebAccess Agent Connections Via SSL

The GroupWise® WebAccess Agent can use the SSL (Secure Socket Layer) protocol to enable secure connections to Post Office Agents (POAs) and the WebAccess Agent Web console. For it to do so, you must ensure that the WebAccess Agent has access to a server certificate file and that you've specified which connections types you want secured through SSL. The following sections provide instructions:

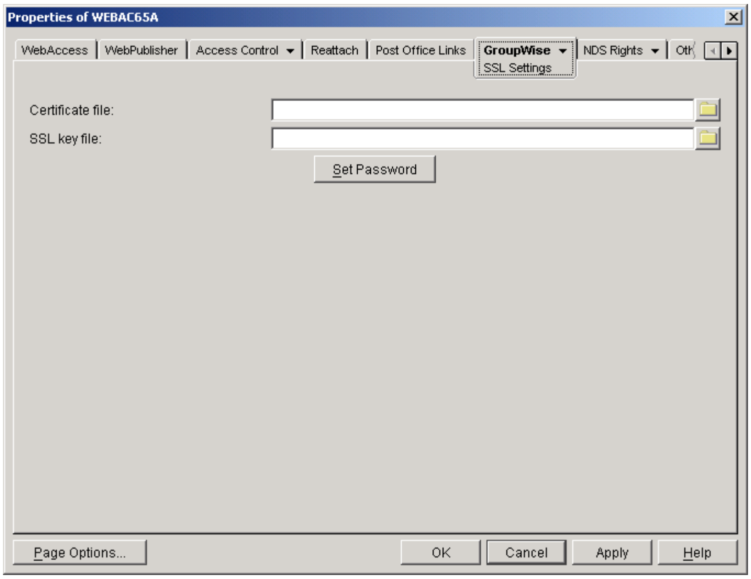
- "Defining the Certificate File" on page 889
- "Defining Which Connections Will Use SSL" on page 890

Defining the Certificate File

To use SSL, the WebAccess Agent requires access to a server certificate file and key file. The WebAccess Agent can use any Base64/PEM or PFX formatted certificate file located on its server. If the WebAccess Agent's server does not have a server certificate file, you can use the GroupWise Generate CSR utility to help you obtain one. For information, see "GroupWise Generate CSR Utility (GWCSRGEN)" on page 79.

To define the certificate file and key file that the WebAccess Agent will use:

1. In ConsoleOne®, right-click the WebAccess Agent object, then click Properties.
2. Click GroupWise > SSL Settings to display the SSL Settings page.



3. Fill in the Certificate File, SSL Key File, and Set Password fields:

Certificate File: Select the server certificate file that the WebAccess Agent will use. The certificate file must be in Base64/PEM or PFX format. If you type the filename rather than using the Browse button to select it, use the full path if the file is not in the same directory as the WebAccess Agent program.

SSL Key File: Select the key file associated with the certificate. If the private key is included in the certificate file rather than in a separate key file, leave this field blank. If you type the filename rather than using the Browse button to select it, use the full path if the file is not in the same directory as the WebAccess Agent program.

Set Password: Click Set Password to specify the password for the key. If the key does not require a password, do not use this option.

4 If you want to define which connections will use SSL, click Apply to save your changes, then continue with the next section, Defining Which Connections Will Use SSL.

or

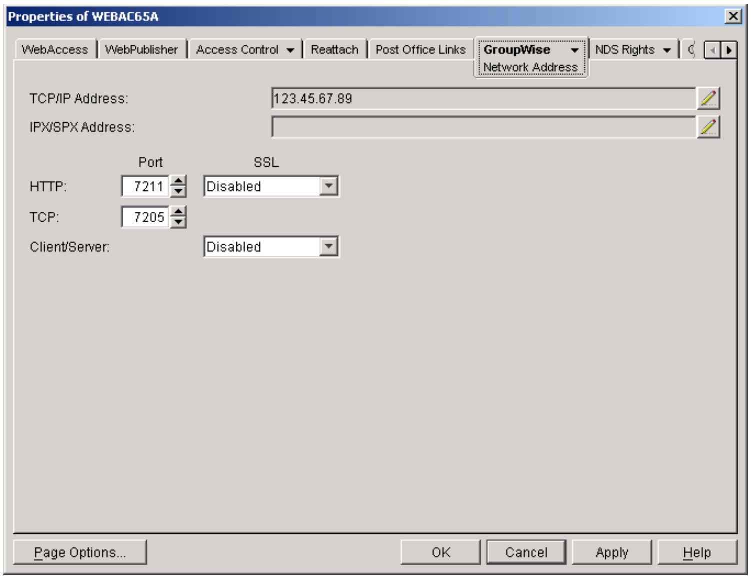
Click OK to save your changes.

Defining Which Connections Will Use SSL

After you've defined the WebAccess Agent's certificate and key file (see "Defining the Certificate File" on page 889), you can configure which connections you want to use SSL.

1 In ConsoleOne, if the WebAccess Agent object's property pages are not already displayed, right-click the WebAccess Agent object, then click Properties.

2 Click GroupWise > Network Address to display the Network Address page.



TCP/IP Address: 123.45.67.89

IPX/SPX Address:

	Port	SSL
HTTP:	7211	Disabled
TCP:	7205	
Client/Server:		Disabled

3 Configure the SSL settings for the following connections:

HTTP: Select Enabled to enable the WebAccess Agent to use a secure connection when passing information to the WebAccess Agent Web console. The Web browser must also be enabled to use SSL; if it is not, a non-secure connection will be used.

Client/Server: Select from the following options to configure the WebAccess Agent's use of secure connections to POAs:

- Disabled: The WebAccess Agent will not support SSL connections. All connections will be non-SSL.
- Enabled: The POA determines whether an SSL connection or non-SSL connection is used.
- Required: The WebAccess Agent will force SSL connections. Non-SSL connections will be denied.

63 Creating a PQA File for the WebAccess Client

You can use the GroupWise® WebAccess Installation program on Windows to create a Web Clipping Application (PQA), also referred to as a Palm Query Application, to enable Palm OS* device users to access their mailboxes through WebAccess.

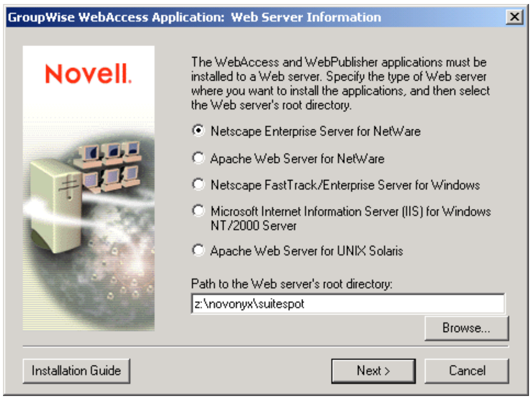
The Web Clipping Application, named groupwise.pqa, includes the URL required to connect to your GroupWise WebAccess installation, a Login page, an About Novell GroupWise page, and the images used when displaying GroupWise WebAccess on the Palm OS device.

To create a groupwise.pqa file:

1 If you've already created another groupwise.pqa file that you want to keep, make sure it is not in the Web server's *doc_root_directory*\com\novell\webacces\palm\en directory. The Installation program overwrites any groupwise.pqa file in the directory.

2 At a Windows workstation, run setup.exe /pqa from the \internet\webacces directory on the *GroupWise 6.5 Administrator* CD or the GroupWise software distribution directory

3 Select the language for the Installation program, then accept the License Agreement to display the following dialog box.



GroupWise WebAccess Application: Web Server Information

The WebAccess and WebPublisher applications must be installed to a Web server. Specify the type of Web server where you want to install the applications, and then select the Web server's root directory.

● Netscape Enterprise Server for NetWare

○ Apache Web Server for NetWare

○ Netscape FastTrack/Enterprise Server for Windows

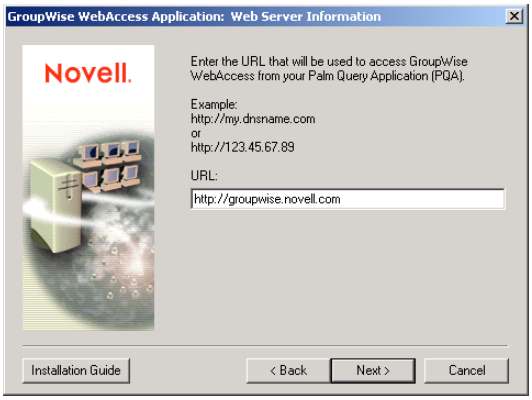
○ Microsoft Internet Information Server (IIS) for Windows NT/2000 Server

○ Apache Web Server for UNIX Solaris

Path to the Web server's root directory:

z:\novonyx\suitespot

4 Select the type of Web server where WebAccess is installed, make sure the path to the Web server's root directory is correct, then click Next.



GroupWise WebAccess Application: Web Server Information

Enter the URL that will be used to access GroupWise WebAccess from your Palm Query Application (PQA).

Example:
http://my.dnsname.com
or
http://123.45.67.89

URL: http://groupwise.novell.com

5 Specify the URL you want included in the .pqa file. For example:

```
http://groupwise.novell.com
```

The Installation program will automatically append /servlet/webacc to the URL so that users will be directed to the WebAccess login page. For example, using the URL above, the Installation program would create the following URL in the groupwise.pqa file:

```
http://groupwise.novell.com/servlet/webacc
```

As you determine the URL, keep in mind the following:

- If the Web server uses SSL, you should change http to https.
- If you are using a proxy server, you need to enter the proxy server's address.
- The Web clipping proxy server (gateway) does not currently support challenge and response authentication. Therefore, you need to ensure that the Web server is not configured to require basic challenge and response authentication, or at least is configured not to require this authentication for the URL defined in the groupwise.pqa file.

6 Click Next to create the .pqa file, then click Finish.

The groupwise.pqa file is created in the Web server's *doc_root_directory*\com\novell\webacces\palm\en directory. You can distribute it to your Palm OS device users just as you would any other .pqa file.

64 Using WebAccess Agent Startup Switches

You can use the switches listed below when starting the GroupWise® WebAccess Agent. The switches override any configuration settings you specified through ConsoleOne®.

To use a switch, you can:

- Add the switch to the command line. For example, load gwinter.nlm /ph-j:\domain\wpgate\webac65a.
- Include the switch in the strtweb.ncf or the strtweb.bat file. The strtweb.ncf file is located in the same directory as the NetWare® WebAccess Agent (typically sys:system) and the strtweb.bat file is located in the same directory as the Windows WebAccess Agent (by default, c:\webacc).
- Include the switch in a startup file and then reference the file when starting the WebAccess Agent. For example:

  ```
  load sys:system\gwinter @webac65a.waa
  ```

  During installation of the WebAccess Agent, the installation program creates a default startup file, *agent_name*.waa, where *agent_name* is the name assigned to the WebAccess Agent (for example, webac65a.waa). The startup file is referenced from the strtweb.ncf and strtweb.bat files and is created in the same directory as the WebAccess Agent.

The following switches are available:

NetWare WebAccess Agent	Linux WebAccess Agent	Windows WebAccess Agent	ConsoleOne Settings
@filename	@filename	@filename	N/A
/cluster	N/A	N/A	N/A
/help	--help	/help	N/A
/home	--home	/home	N/A
/http	--http	/http	GroupWise > Network Address
/httpuser	--httpuser	/httpuser	GroupWise > Optional Gateway Settings > HTTP User Name
/httppassword	--httppassword	/httppassword	GroupWise > Optional Gateway Settings > HTTP Password
/ip	--ip	/ip	GroupWise > Network Address
/log	--log	/log	GroupWise > Log Files > Log File Path
/logdays	--logdays	/logdays	GroupWise > Log Files > Max Log File Age

NetWare WebAccess Agent	Linux WebAccess Agent	Windows WebAccess Agent	ConsoleOne Settings
/logdiskon	--logdiskon	/logdiskon	N/A
/loglevel	--loglevel	/loglevel	GroupWise > Log Settings > Logging Level
/logmax	--logmax	/logmax	GroupWise > Log Settings > Max Log Disk Space
/maxusers	--maxusers	/maxusers	N/A
/password	N/A	N/A	N/A
/port	--port	/port	GroupWise > Network Address
N/A	--show	N/A	N/A
/threads	--threads	/threads	WebAccess > Settings > Maximum Threads
/user	N/A	N/A	N/A
/work	--work	/work	

@filename

Specifies a startup file to use. You can add any of the WebAccess Agent startup switches to the startup file and then reference the file when starting the WebAccess Agent. For example:

```
load sys:system\gwinter @webac65a.waa
```

During installation of the WebAccess Agent, the Installation program creates a default startup file, *agent_name*.waa, where *agent_name* is the name assigned to the WebAccess Agent (for example, webac65a.waa). On NetWare and Windows, the *agent_name*.waa file is created in the same directory as the WebAccess Agent program. On Linux, it is created in the /opt/novell/groupwise/agents/share directory

The startup file is referenced from the strtweb.ncf file on NetWare, the grpwise-wa script on Linux, and the strtweb.bat file on Windows, which enables you to run strtweb.ncf, grpwise-wa, or strtweb.bat to start the WebAccess Agent.

/cluster

Enables the WebAccess Agent to run in a clustered environment (using Novell® Cluster Services™).

For detailed information about running the WebAccess Agent in a clustered environment, see “Implementing WebAccess in a Novell Cluster” in “Novell Cluster Services” in the *GroupWise 6.5 Interoperability Guide*.

/help

Displays a listing and description of the startup switches.

/home (Required)

Specifies the path to the WebAccess Agent's gateway directory under the domain directory. If you use the default WebAccess Agent gateway directory name, the path is *x*:\domain\wpgate\webac65a. This switch is required.

/http

If the WebAccess Agent's Web console is disabled in ConsoleOne, this switch enables the Web console and assigns the port you specify. The default port is 7211.

/httpuser

Specifies the username that must be entered when logging in to the WebAccess Agent's Web console.

/httppassword

Specifies the password that must be entered when logging in to the WebAccess Agent's Web console.

/ip

Specifies the IP address of the WebAccess Agent's server.

/log

Specifies the path to the log file directory. On NetWare and Windows, the default log file directory is the *domain*\wpgate\webac65a\000.prc directory. On Linux, the default directory is /var/log/novell/groupwise/*domain.gateway*/000.prc.

Log files are named *mmdd.nnn*, where *mm* is the month, *dd* is the day, and *nnn* is a sequenced number starting with 001. For example, the first log file used on March 28 is named 0328.001, and the second log file used is named 0328.002.

For more information about the WebAccess Agent's logging, see "Controlling the Agent's Logging" on page 832.

/logdays

Specifies the maximum number of days to keep log files. This setting works in combination with the /logmax setting. Log files are deleted when the maximum number of days or disk space size is reached, whichever comes first. The default is 7 days.

For more information about the WebAccess Agent's logging, see "Controlling the Agent's Logging" on page 832.

/logdiskon

Turns disk logging on. By default, the log file is not written to disk on NetWare and Windows. On Linux, the log file is written to disk by default.

For more information about the WebAccess Agent's logging, see "Controlling the Agent's Logging" on page 832.

/loglevel

Specifies the level of information to write to the screen and to disk. There are three levels: Normal, Verbose, and Diagnostic. The default level is Normal. You can use Verbose to receive more information. You should use Diagnostic only if you are having problems with the WebAccess Agent. The verbose and diagnostic logging levels do not degrade Internet Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use. For more information about the logging levels, see "Controlling the Agent's Logging" on page 832.

/logmax

Specifies the maximum disk space to use for logging. This setting works in combination with the /logdays setting. Log files are deleted when the maximum disk space or number of days is reached, whichever comes first. The default is 1024 KB.

For more information about the WebAccess Agent's logging, see "Controlling the Agent's Logging" on page 832.

/maxusers

Specifies the maximum number of users that the WebAccess Agent will allow to log in at one time. The default is 250.

/password (NetWare Only)

Used by the NetWare WebAccess Agent only. Specifies the Novell eDirectory™ password to use to access the network servers where the GroupWise domain directory and post office directories reside. Must be used with "/user (NetWare Only)" on page 899.

/port-*number*

Specifies the port number the WebAccess Agent listens to. The default is 7205.

--show

Used by the Linux WebAccess Agent only. Running the WebAccess Agent with this option disabled (the default) causes the WebAccess Agent to run as a daemon without a user interface. Enabling this option causes the logging UI to appear in a terminal window.

/threads-*number*

Specifies the number of threads the WebAccess Agent uses to process user requests. The default is 12, which means the WebAccess Agent can process 12 user requests at one time. For more information, see "Configuring the WebAccess Agent" on page 829.

/user (NetWare Only)

Used by the NetWare WebAccess Agent only. Specifies the eDirectory username to use to access the network servers where the GroupWise domain directory and post office directories reside. Must be used with /password.

/work

Specifies the path to the WebAccess Agent's work directory. By default, the work directory is the same as the WebAccess Agent's gateway directory (*x*:\domain\wpgate\webac65a).

XIII Monitor

65 Starting the Monitor Agent

Detailed instructions for installing and starting the GroupWise® Monitor Agent for the first time are provided in "Installing GroupWise Monitor" in the *GroupWise 6.5 Installation Guide*. This section presents some additional Monitor Agent startup information.

- "Starting the Linux Monitor Agent" on page 903
- "Starting the Windows Monitor Agent" on page 905

Starting the Linux Monitor Agent

- "Starting the Linux Monitor Agent Manually" on page 903
- "Starting the Linux Monitor Agent Automatically" on page 904
- "Stopping the Linux Monitor Agent" on page 904

Starting the Linux Monitor Agent Manually

You do not need to be logged in as root to start the Monitor Agent.

1. Make sure you are logged in as root.
2. Make sure you know the path to a domain directory where a domain database (wpdomain.db) is located or the IP address of a server where the MTA is running.
3. Change to the GroupWise agent bin directory.

   ```
   cd /opt/novell/groupwise/agents/bin
   ```

4. Use one of the following commands to start the Monitor Agent:

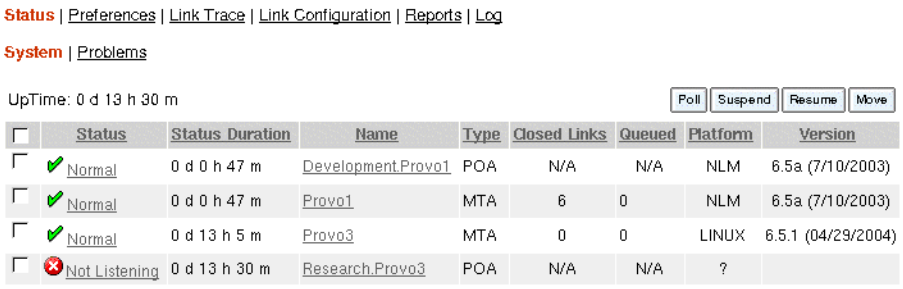
   ```
   ./gwmon --home /domain_directory &
   ./gwmon --ipa IP_address --ipp port_number &
   ```

   A message indicates that the Monitor Agent is polling the domain you specified. The Monitor Agent does not have a --show switch to provide a user interface.

   You can also start the Monitor Agent using its startup script (/etc/initd/grpwise-ma).

5. View the following URL to verify that the Monitor Agent is running:

   http://localhost:8200



Status | Preferences | Link Trace | Link Configuration | Reports | Log
System | Problems
Poll
Suspend
Resume
Move

UpTime: 0 d 13 h 30 m

☐	Status	Status Duration	Name	Type	Closed Links	Queued	Platform	Version
☐	✓ Normal	0 d 0 h 47 m	Development.Provo1	POA	N/A	N/A	NLM	6.5a (7/10/2003)
☐	✓ Normal	0 d 0 h 47 m	Provo1	MTA	6	0	NLM	6.5a (7/10/2003)
☐	✓ Normal	0 d 13 h 5 m	Provo3	MTA	0	0	LINUX	6.5.1 (04/29/2004)
☐	✖ Not Listening	0 d 13 h 30 m	Research.Provo3	POA	N/A	N/A	?	

Status information for the agents in your GroupWise system is displayed.

Starting the Linux Monitor Agent Automatically

If you selected Launch Monitor Agent on System Startup in the Monitor Agent Installation program, your system was configured so that the Monitor Agent would start automatically. The Monitor Installation program always creates a grpwise-ma startup script in /etc/init.d for starting the Monitor Agent. To enable automatic startup, the Monitor Installation program creates symbolic links named S99grpwise-ma in the rc3.d and rc5.d directories so that the Monitor Agent can load on startup into runlevel 3 or 5, depending on the configuration of your Linux system.

When the grpwise-ma script runs and starts the Monitor Agent, it reads the Monitor Agent configuration file (monitor.xml) in /opt/novell/groupwise/agents/share to check for configuration information.

Stopping the Linux Monitor Agent

NOTE: If you started the Monitor Agent as root, then you must be logged in as root in order to stop it.

When you start the Monitor Agent with the grpwise-ma startup script, you can also use the script to stop it.

1. Change to the /etc/init.d directory.
2. To stop the Monitor Agent, enter the following command:

   ```
   ./grpwise-ma stop
   ```
3. To confirm that the Monitor Agent has stopped, enter the following command:

   ```
   ./grpwise-ma status
   ```

When you start the Monitor Agent manually (without using the grpwise-ma script), use the standard Linux kill command to stop it.

1. Determine the process ID of the Monitor Agent.

   ```
   ps -eaf | grep gwmon
   ```

   The PIDs for all gwmon processes are listed.
2. Kill the first gwmon process in the list.

   ```
   kill first_process_ID
   ```

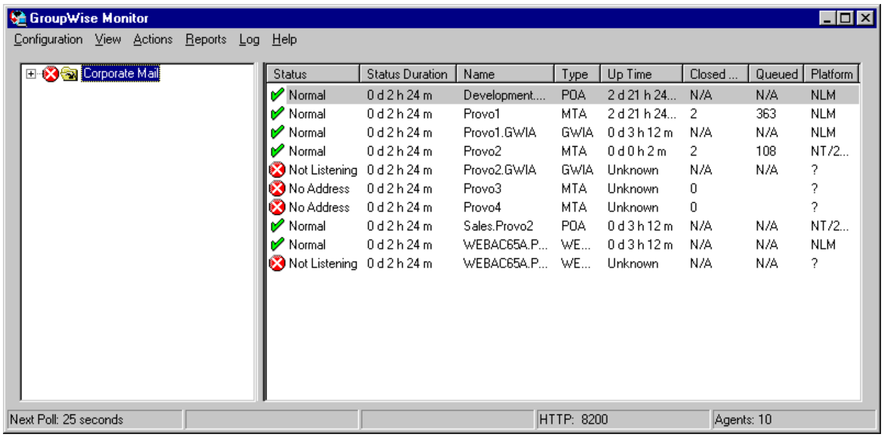
   It might take a few seconds for all gwmon processes to terminate.
3. Repeat the ps command to verify that the Monitor Agent stopped.

Starting the Windows Monitor Agent

Starting the Windows Monitor Agent Manually

In Windows, click Start > Programs > GroupWise Monitor > GroupWise Monitor. You might also want to create a desktop icon for it.

The Monitor Agent console appears.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 2 h 24 m	Development....	POA	2 d 21 h 24...	N/A	N/A	NLM
✓ Normal	0 d 2 h 24 m	Provo1	MTA	2 d 21 h 24...	2	363	NLM
✓ Normal	0 d 2 h 24 m	Provo1.GWIA	GWIA	0 d 3 h 12 m	N/A	N/A	NLM
✓ Normal	0 d 2 h 24 m	Provo2	MTA	0 d 0 h 2 m	2	108	NT/2...
☒ Not Listening	0 d 2 h 24 m	Provo2.GWIA	GWIA	Unknown	N/A	N/A	?
☒ No Address	0 d 2 h 24 m	Provo3	MTA	Unknown	0		?
☒ No Address	0 d 2 h 24 m	Provo4	MTA	Unknown	0		?
✓ Normal	0 d 2 h 24 m	Sales.Provo2	POA	0 d 3 h 12 m	N/A	N/A	NT/2...
✓ Normal	0 d 2 h 24 m	WEBAC65A.P...	WE...	0 d 3 h 12 m	N/A	N/A	NLM
☒ Not Listening	0 d 2 h 24 m	WEBAC65A.P...	WE...	Unknown	N/A	N/A	?

Next Poll: 25 seconds | HTTP: 8200 | Agents: 10

If the Monitor Agent console does not appear, see "Monitor Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Starting the Windows Monitor Agent Automatically

To start the Monitor Agent automatically whenever you restart the Windows server, you can add the Monitor Agent program to the Windows Startup group.

1. In Windows NT, click Start > Settings > Taskbar > Start Menu Programs > Add.

   or

   In Windows 2000, click Start > Settings > Taskbar & Start Menu > Advanced > Add.
2. Browse to the directory where you installed the Monitor Agent.
3. Double-click gwmon.exe.
4. Click Next.
5. Select the Startup folder, provide a name for the shortcut, then click Finish.
6. If possible, restart the server to verify that the Monitor Agent starts when you log in.

Stopping the Windows Monitor Agent

At the Monitor Agent console:

1 Click File > Exit.

or

Close the window where the Monitor Agent is running.

Understanding the Monitor Agent Consoles

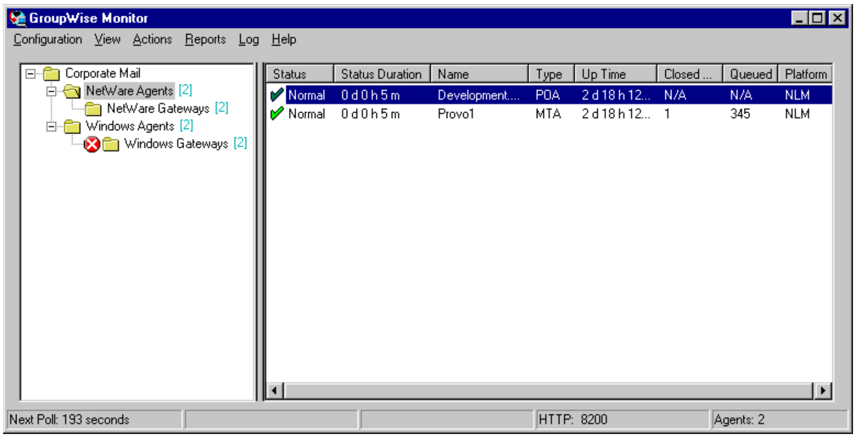
The Monitor Agent offers three consoles:

- "Monitor Agent Console" on page 906
- "Monitor Agent Web Console" on page 906
- "Monitor Web Console" on page 907

For a comparison of the capabilities of the three consoles, see Chapter 70, "Comparing the Monitor Agent Consoles," on page 953

Monitor Agent Console

The Monitor Agent console is available for the Windows Monitor Agent but not for the Linux Monitor Agent.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 0 h 5 m	Development....	POA	2 d 18 h 12...	N/A	N/A	NLM
✓ Normal	0 d 0 h 5 m	Provo1	MTA	2 d 18 h 12...	1	345	NLM

Next Poll: 193 seconds

HTTP: 8200

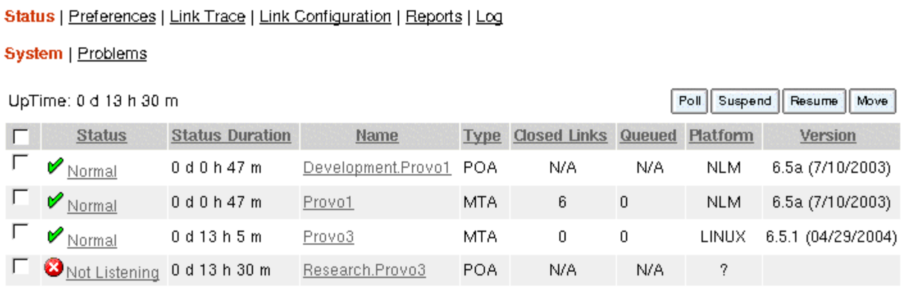
Agents: 2

All agent configuration tasks can be performed at the Monitor Agent console, but some reports are not available.

Monitor Agent Web Console

The Monitor Agent Web console is platform-independent and can be viewed at the following URL:

http://*Web_server_address*:8200



Status | Preferences | Link Trace | Link Configuration | Reports | Log

System | Problems

UpTime: 0 d 13 h 30 m

□	Status	Status Duration	Name	Type	Closed Links	Queued	Platform	Version
□	✓ Normal	0 d 0 h 47 m	Development.Provo1	POA	N/A	N/A	NLM	6.5a (7/10/2003)
□	✓ Normal	0 d 0 h 47 m	Provo1	MTA	6	0	NLM	6.5a (7/10/2003)
□	✓ Normal	0 d 13 h 5 m	Provo3	MTA	0	0	LINUX	6.5.1 (04/29/2004)
□	☒ Not Listening	0 d 13 h 30 m	Research.Provo3	POA	N/A	N/A	?	

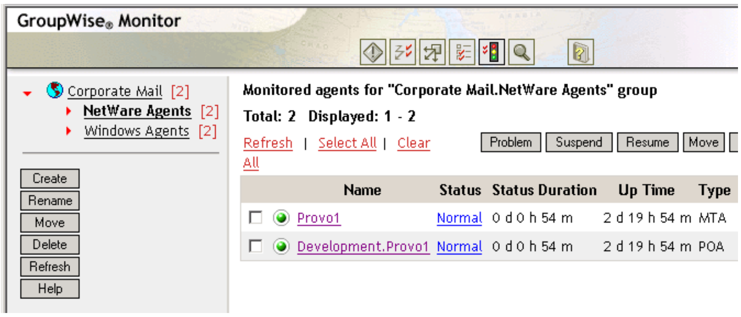
To create the Monitor Agent Web console display, your Web server communicates directly with the Monitor Agent to obtain agent status information. You must be behind your firewall to use the Monitor Agent Web console. Because the Linux Monitor Agent does not have a console on the server where it runs, you use the Monitor Agent Web console in its place on Linux.

Several Monitor features are available at the Monitor Agent Web console that are not available at the Monitor Agent server console or the Monitor Web console. These are summarized in Chapter 70, "Comparing the Monitor Agent Consoles," on page 953.

Monitor Web Console

The Monitor Web console is also platform-independent and can be viewed at the following URLs:

Linux: http://*network_address*/gwmon/gwmonitor
Windows: https://*network_address*/servlet/gwmonitor



Monitored agents for "Corporate Mail.NetWare Agents" group

Total: 2 Displayed: 1 - 2

	Name	Status	Status Duration	Up Time	Type
□ ●	Provo1	Normal	0 d 0 h 54 m	2 d 19 h 54 m	MTA
□ ●	Development.Provo1	Normal	0 d 0 h 54 m	2 d 19 h 54 m	POA

To create the Monitor Web console display, your Web server communicates with the Monitor Application (a component of your Web server), which then communicates with the Monitor Agent to obtain agent status information. This enables the Monitor Web console to be available outside your firewall, while the Monitor Agent Web console can be used only inside your firewall.

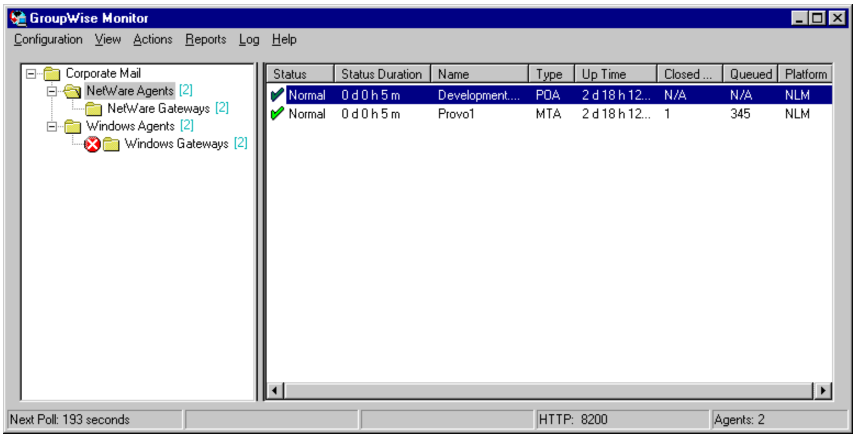
The Monitor Web console is divided into the Agent Groups window on the left and the Agent Status window on the right. Using the Agents Groups window, you can create and manage agent groups the same as you can at the Monitor Agent server console.

The Monitor Web console does not include some features that are available at the Monitor Agent server console and the Monitor Agent Web console. These are summarized in Chapter 70, "Comparing the Monitor Agent Consoles," on page 953.

66 Configuring the Monitor Agent

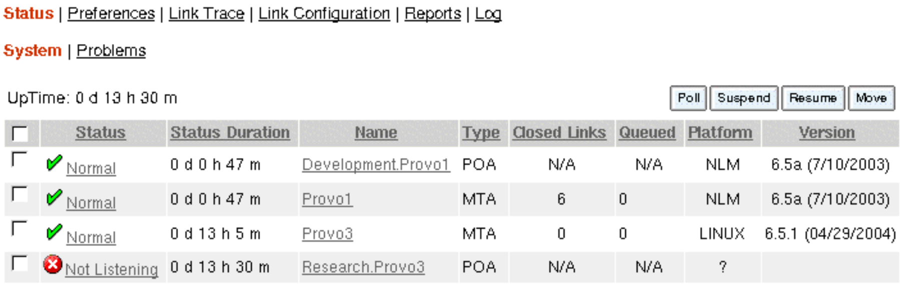
The default configuration of the GroupWise® Monitor Agent is adequate to begin monitoring existing GroupWise agents (POAs, MTAs, Internet Agents, and WebAccess Agents). You can also customize the configuration to meet your specific monitoring needs.

On Windows, you configure the Monitor Agent at the Monitor Agent console on the Windows server where the Monitor Agent is running.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 0 h 5 m	Development....	POA	2 d 18 h 12...	N/A	N/A	NLM
✓ Normal	0 d 0 h 5 m	Provo1	MTA	2 d 18 h 12...	1	345	NLM

On Linux, similar functionality is available in your Web browser at http://localhost:8200.


Status | Preferences | Link Trace | Link Configuration | Reports | Log
System | Problems
Poll
Suspend
Resume
Move

UpTime: 0 d 13 h 30 m

□	Status	Status Duration	Name	Type	Closed Links	Queued	Platform	Version
□	✓ Normal	0 d 0 h 47 m	Development.Provo1	POA	N/A	N/A	NLM	6.5a (7/10/2003)
□	✓ Normal	0 d 0 h 47 m	Provo1	MTA	6	0	NLM	6.5a (7/10/2003)
□	✓ Normal	0 d 13 h 5 m	Provo3	MTA	0	0	LINUX	6.5.1 (04/29/2004)
□	☒ Not Listening	0 d 13 h 30 m	Research.Provo3	POA	N/A	N/A	?	

The following topics help you customize the Monitor Agent for your specific needs:

- "Selecting Agents to Monitor" on page 910
- "Creating and Managing Agent Groups" on page 912
- "Configuring Monitoring Protocols" on page 914
- "Configuring Polling of Monitored Agents" on page 917
- "Configuring E-Mail Notification of Agent Problems" on page 918
- "Configuring Audible Notification of Agent Problems" on page 922

- “Configuring SNMP Trap Notification of Agent Problems” on page 923
- “Configuring Authentication and Intruder Lockout for the Monitor Web Console” on page 924
- “Configuring Proxy Service Support for the Monitor Web Console” on page 925
- “Configuring Monitor Agent Log Settings” on page 925

Selecting Agents to Monitor

By default, the Monitor Agent starts monitoring all GroupWise agents (POAs, MTAs, Internet Agents, and WebAccess Agents) in your GroupWise system, based on the information from a domain database (wpdomain.db). You might not want to continue monitoring all agents. And as your GroupWise system grows, you might want to monitor additional agents.

- “Filtering the Agent List” on page 910
- “Adding All Agents on a Server” on page 911
- “Adding All Agents on a Subnet” on page 911
- “Adding an Individual Agent” on page 911
- “Removing Added Agents” on page 912

Filtering the Agent List

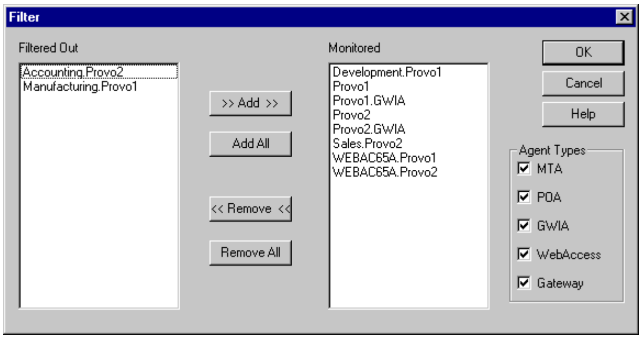
You can configure the Monitor Agent to stop and start monitoring selected agents as needed.

At the Windows Monitor Agent console:

1. Click Configuration > Filter.

   or

   On Linux, click Preferences > Filter.



Filtered Out:
Accounting.Provo2
Manufacturing.Provo1

Monitored:
Development.Provo1
Provo1
Provo1.GWIA
Provo2
Provo2.GWIA
Sales.Provo2
WEBAC65A.Provo1
WEBAC65A.Provo2

Agent Types
☑ MTA
☑ POA
☑ GWIA
☑ WebAccess
☑ Gateway

   The Filtered Out list displays all agents that are not currently being monitored.

2. Select one or more agents in the Monitored list, then click Remove to move them to the Filtered Out list.
3. Click OK.

Agents in the Filtered Out list are not monitored and do not appear at the Monitor Agent console nor at the Monitor Web console. To start monitoring a filtered-out agent, move it back to the Monitored list.

Adding All Agents on a Server

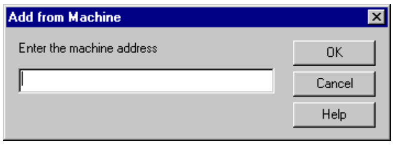
If you add a new server to your GroupWise system or want to monitor agents in a different GroupWise system, you can easily start monitoring all the agents running on that server.

At the Windows Monitor Agent console:

1 Click Configuration > Add from Server.

  or

  On Linux, click Preferences > Add Agents.



2 Type the IP address of the new server, then click OK.

  All GroupWise agents on the new server are added to the list of monitored agents.

If the server is part of your local GroupWise system, you can simply restart the Monitor Agent and it picks up all new agents in your system.

Adding All Agents on a Subnet

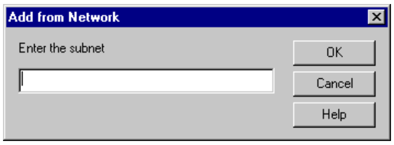
If you add several new servers to your GroupWise system or want to monitor agents in a different GroupWise system, you can easily start monitoring all the agents running on the same subnet.

At the Windows Monitor Agent console:

1 Click Configuration > Add from Network.

  or

  On Linux, click Preferences > Add Agents.



2 Type the subnet portion of the IP addresses of the new servers, then click OK.

  All GroupWise agents on the subnet are added to the list of monitored agents.

If the servers are part of your local GroupWise system, you can simply restart the Monitor Agent and it picks up all new agents in your system.

Adding an Individual Agent

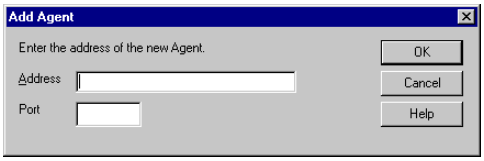
You can start monitoring an individual agent anywhere in your GroupWise system or another GroupWise system.

At the Windows Monitor Agent console:

1 Click Configuration > Add Agent.

or

On Linux, click Preferences > Add Agents.



Enter the address of the new Agent.

2 Type the IP address of the server where the agent runs.

3 Type the port number the agent listens on.

4 Click OK.

The agent is added to the list of monitored agents.

Removing Added Agents

To stop monitoring agents that you have manually added to the Monitor Agent's configuration:

At the Windows Monitor Agent console:

1 Click Configuration > Remove Agents.

or

On Linux, click Preferences > Remove Agents.

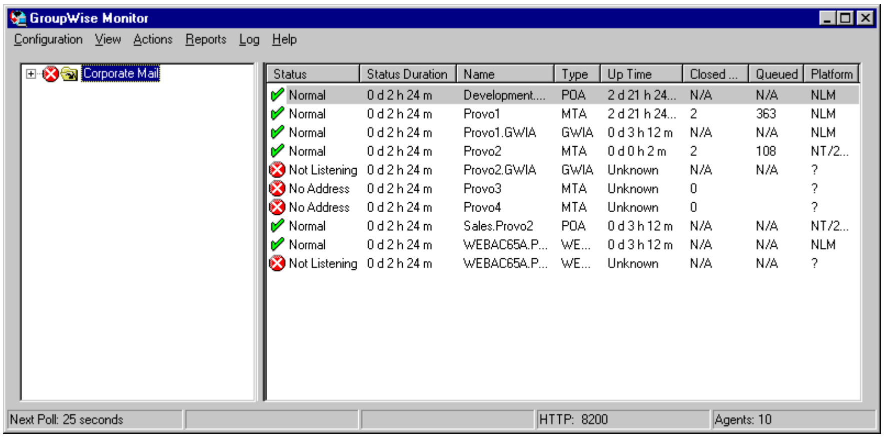
2 Select the agents you want to remove, then click Remove.

3 Click OK.

Creating and Managing Agent Groups

You might find it convenient to group related agents together for monitoring purposes. Initially, all agents are in a single group with the same name as your GroupWise system.

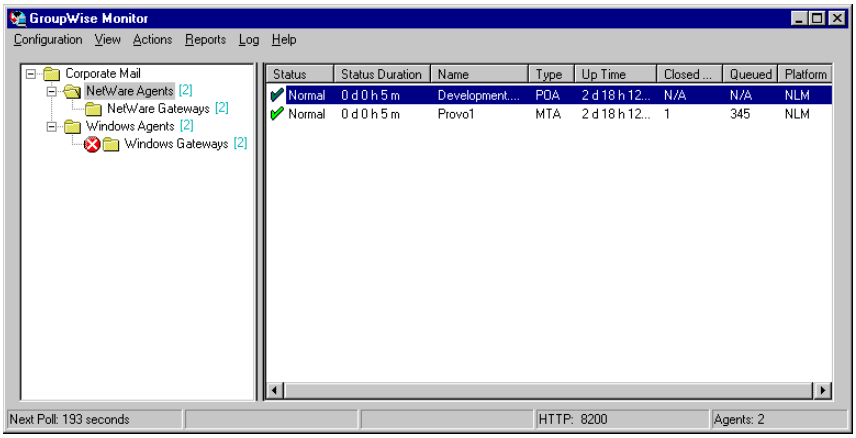
Agent groups are displayed on the left side of the Monitor Agent console. When you select an agent group, the monitored agents in the group and their status information are listed on the right side of the Monitor Agent console.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 2 h 24 m	Development....	POA	2 d 21 h 24...	N/A	N/A	NLM
✓ Normal	0 d 2 h 24 m	Provo1	MTA	2 d 21 h 24...	2	363	NLM
✓ Normal	0 d 2 h 24 m	Provo1.GWIA	GWIA	0 d 3 h 12 m	N/A	N/A	NLM
✓ Normal	0 d 2 h 24 m	Provo2	MTA	0 d 0 h 2 m	2	108	NT/2...
☒ Not Listening	0 d 2 h 24 m	Provo2.GWIA	GWIA	Unknown	N/A	N/A	?
☒ No Address	0 d 2 h 24 m	Provo3	MTA	Unknown	0		?
☒ No Address	0 d 2 h 24 m	Provo4	MTA	Unknown	0		?
✓ Normal	0 d 2 h 24 m	Sales.Provo2	POA	0 d 3 h 12 m	N/A	N/A	NT/2...
✓ Normal	0 d 2 h 24 m	WEBAC65A.P...	WE...	0 d 3 h 12 m	N/A	N/A	NLM
☒ Not Listening	0 d 2 h 24 m	WEBAC65A.P...	WE...	Unknown	N/A	N/A	?

Next Poll: 25 seconds HTTP: 8200 Agents: 10

You can create additional groups and subgroups as needed to make monitoring similar agents easier. You might want to create agent groups based on geographical areas, on administrative responsibilities, or on agent configuration similarities. The number of agents in the group is displayed to the right of the group name in the agent groups window.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 0 h 5 m	Development....	POA	2 d 18 h 12...	N/A	N/A	NLM
✓ Normal	0 d 0 h 5 m	Provo1	MTA	2 d 18 h 12...	1	345	NLM

In addition, by creating agent groups, you can provide configuration settings for monitoring just once for all agents in each group, rather than having to provide them individually for each agent in your GroupWise system.

- "Creating an Agent Group" on page 913
- "Managing Agent Groups" on page 913
- "Viewing Your Agent Group Hierarchy" on page 914
- "Configuring an Agent Group" on page 914

NOTE: On Linux, perform these tasks in the Monitor Web console.

Creating an Agent Group

At the Windows Monitor Agent console:

1. Right-click the folder where you want to create the agent group, then click Create.
2. Type a name for the group, then click OK to create a new folder for the agent group.

   The group name must be unique within its parent group.
3. Click a folder containing agents that you want to add to the new group.
4. Drag and drop agents into the new group as needed.
5. Click the new group to view its contents.

You can nest groups within groups as needed.

Managing Agent Groups

Managing agent groups is easy:

- To rename an agent group, right-click the agent group, click Rename, type the new name, then press Enter.
- To move an agent group, drag and drop it to its new location.

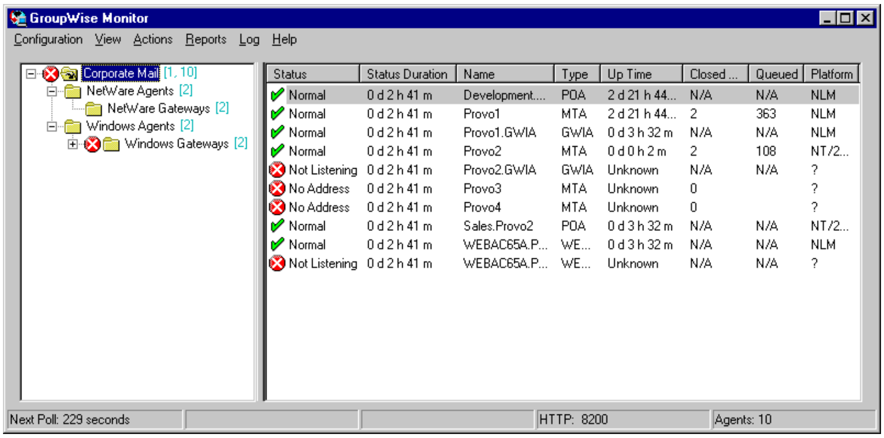
- To delete an agent group, right-click the agent group, then click Delete. A group must be empty before you can delete it.

Viewing Your Agent Group Hierarchy

When you create nested groups, you can choose how much of the hierarchy you want displayed:

- You can open and close groups manually by clicking the plus and minus icons beside each folder.
- To expand your entire group hierarchy, click View > Expand Tree.
- To collapse your entire group hierarchy, click View > Collapse Tree.

You can also decide, when viewing the agents in a group, whether you want to view just the agents in the currently selected group or the agents in subgroups as well. By default, only the agents in the selected folder are listed in the agent window. Right-click an agent group, then click Show Subgroup Agents to display the contents of nested groups along with the selected group.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 2 h 41 m	Development....	POA	2 d 21 h 44...	N/A	N/A	NLM
✓ Normal	0 d 2 h 41 m	Provo1	MTA	2 d 21 h 44...	2	363	NLM
✓ Normal	0 d 2 h 41 m	Provo1.GWIA	GWIA	0 d 3 h 32 m	N/A	N/A	NLM
✓ Normal	0 d 2 h 41 m	Provo2	MTA	0 d 0 h 2 m	2	108	NT/2...
☒ Not Listening	0 d 2 h 41 m	Provo2.GWIA	GWIA	Unknown	N/A	N/A	?
☒ No Address	0 d 2 h 41 m	Provo3	MTA	Unknown	0		?
☒ No Address	0 d 2 h 41 m	Provo4	MTA	Unknown	0		?
✓ Normal	0 d 2 h 41 m	Sales.Provo2	POA	0 d 3 h 32 m	N/A	N/A	NT/2...
✓ Normal	0 d 2 h 41 m	WEBAC65A.P...	WE...	0 d 3 h 32 m	N/A	N/A	NLM
☒ Not Listening	0 d 2 h 41 m	WEBAC65A.P...	WE...	Unknown	N/A	N/A	?

Next Poll: 229 seconds | HTTP: 8200 | Agents: 10

Numbers in brackets beside each group indicate the number of agents in the selected group and the total number displayed

Configuring an Agent Group

Configuration settings for monitoring can be set for each monitored agent individually, for each agent group, or for all monitored agents collectively. You can establish default configuration settings for all agents by setting them on the root agent group that is named the same as your GroupWise system. Those default settings can be inherited by each subgroup that you create thereafter if you select Apply Options to Subgroups. Those default settings can be overridden by establishing different settings for an agent group or for an individual agent if you deselect Use Parent Options.

Configuring Monitoring Protocols

By default, the Monitor Agent uses HTTP to communicate with the agents it monitors, whenever HTTP is available. If HTTP is not available, the Monitor Agent changes automatically to SNMP.

GroupWise 6.*x* agents and gateways as well as the GroupWise agents provided with the GroupWise 5.5 Enhancement Pack can be monitored using HTTP. Agents dating from GroupWise 5.5 and earlier, as well as 5.5-level GroupWise gateways, must be monitored using SNMP.

- "Configuring the Monitor Agent for HTTP" on page 915
- "Configuring the Monitor Agent for SNMP" on page 916

Configuring the Monitor Agent for HTTP

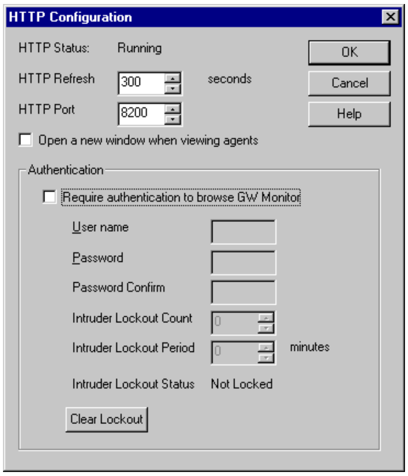
You can customize how the Monitor Agent communicates with your Web browser.

At the Windows Monitor Agent console:

1 Click Configuration > HTTP.

or

On Linux, click Preferences > Setup, then scroll down to the HTTP Settings section.



HTTP Status: Running

HTTP Refresh 300 seconds

HTTP Port 8200

☐ Open a new window when viewing agents

☐ Require authentication to browse GW Monitor

User name

Password

Password Confirm

Intruder Lockout Count 0

Intruder Lockout Period 0 minutes

Intruder Lockout Status Not Locked

2 Modify the HTTP settings as needed:

HTTP Refresh: Specify the number of seconds after which the Monitor Agent sends updated information to the Monitor Web console. The default is 300 seconds (5 minutes).

HTTP Port: Specify the port number for the Monitor Agent to listen on for requests for information from the Web console. The default port number is 8200.

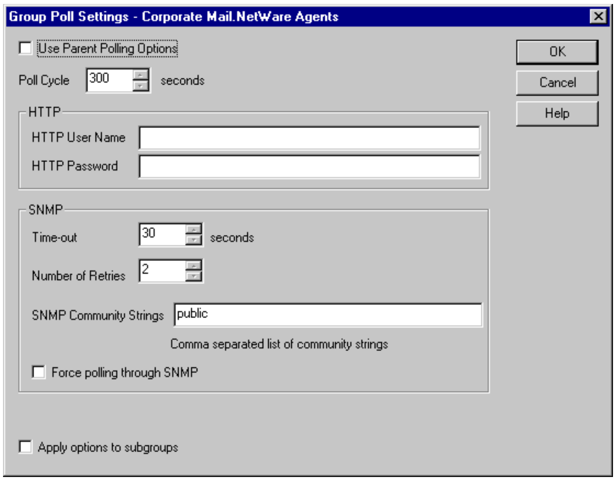
Open a New Window When Viewing Agents: Select this option to open a new Web browser window whenever you display an agent Web console. This enables you to view the Monitor Web console and an agent Web console at the same time, or to view two agent Web consoles at the same time for comparison.

3 Click OK to put the new HTTP settings into effect.

4 Click Configuration > Poll Settings.

or

On Linux, click Preferences > Setup, then scroll down to the HTTP Settings section.



Group Poll Settings - Corporate Mail.NetWare Agents

☐ Use Parent Polling Options

Poll Cycle 300 seconds

HTTP

HTTP User Name

HTTP Password

SNMP

Time-out 30 seconds

Number of Retries 2

SNMP Community Strings public

Comma separated list of community strings

☐ Force polling through SNMP

☐ Apply options to subgroups

5 Fill in the following fields:

Poll Cycle: Specify the number of seconds after which the Monitor Agent polls all monitored GroupWise agents for updated information.

By default, the Monitor Agent starts 20 threads to poll monitored agents. You can use the /pollthreads startup switch to adjust the number of threads.

By default, the Monitor Agent communicates with other GroupWise agents by way of XML. However, if XML is unavailable, the Monitor Agent automatically uses SNMP instead. Prior to the GroupWise 5.5 Enhancement Pack, GroupWise agents did not support XML, so the Monitor Agent must use SNMP to monitor these older agents. If you need to monitor older agents, see "Configuring the Monitor Agent for SNMP" on page 916.

If all monitored agents in the group require the same username and password in order to communicate with the Monitor Agent, you can provide that information as part of the Monitor Agent's configuration.

HTTP User Name: Provide the username for the Monitor Agent to use when contacting monitored agents in the group for status information.

HTTP Password: Provide the password, if any, associated with the username specified in the field above.

NOTE: On Linux, the HTTP User Name and HTTP Password fields are not available. However, you can use the --httpagentuser and --httpagentpassword startup switches on the command line when you start the Monitor Agent to achieve the same functionality.

If the monitored agents use different usernames and passwords, you are prompted to supply them when the Monitor Agent needs to communicate with the monitored agents.

6 Click Apply Options to Subgroups if you want subgroups to inherit these settings.

7 Click OK to put the specified poll cycle into effect.

Configuring the Monitor Agent for SNMP

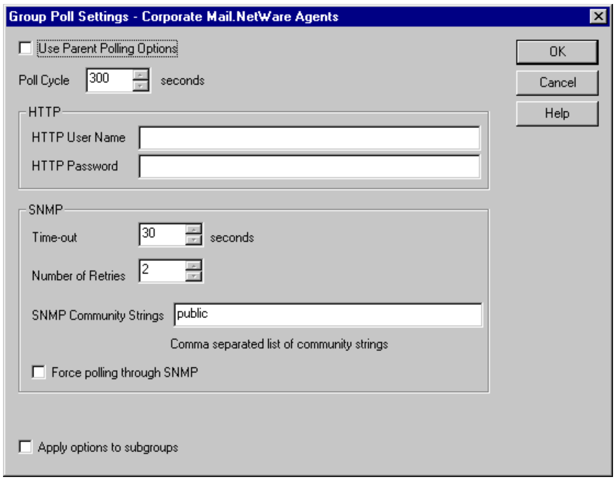
The Monitor Agent must use SNMP to communicate with GroupWise agents that date from earlier than the GroupWise 5.5 Enhancement Pack. You can customize how the Monitor Agent communicates with such older agents and how it communicates with SNMP monitoring and management programs.

At the Windows Monitor Agent console:

1 Click Configuration > Polling.

or

On Linux, click Preferences > Setup, then scroll down to the SNMP Settings section.



Group Poll Settings - Corporate Mail.NetWare Agents

☐ Use Parent Polling Options

Poll Cycle 300 seconds

HTTP

HTTP User Name

HTTP Password

SNMP

Time-out 30 seconds

Number of Retries 2

SNMP Community Strings public

Comma separated list of community strings

☐ Force polling through SNMP

☐ Apply options to subgroups

2 Specify the number of seconds after which the Monitor Agent polls all monitored GroupWise agents for updated information using SNMP.

3 In the SNMP box, modify the SNMP settings as needed:

Time Out: Specify the number of seconds the Monitor Agent should wait for a response from servers where GroupWise agents run.

Number of Retries: Specify how often the Monitor Agent should try to contact the servers where GroupWise agents run.

SNMP Community Strings: Provide a comma-delimited list of community strings required to access the servers where GroupWise agents run.

Force Polling through SNMP: Select this option to use SNMP polling instead of the default of XML polling when contacting servers where agents in the group run.

4 Click Apply Options to Subgroups if you want subgroups to inherit these settings.

5 Click OK to put the new SNMP settings into effect.

6 Make sure the GroupWise agents you want to monitor using SNMP are enabled for SNMP. See "Setting Up SNMP Services for the POA" on page 499 and "Setting Up SNMP Services for the MTA" on page 627. The same instructions can be followed for all GroupWise 5.*x* and 6.*x* agents.

Configuring Polling of Monitored Agents

By default, the Monitor Agent polls all monitored agents every five minutes. You can adjust the poll cycle as needed.

At the Windows Monitor Agent console:

1 Select the root agent group to set the poll cycle default for all monitored agents.

or

Select any agent group to set the poll cycle for the agents in the selected group.

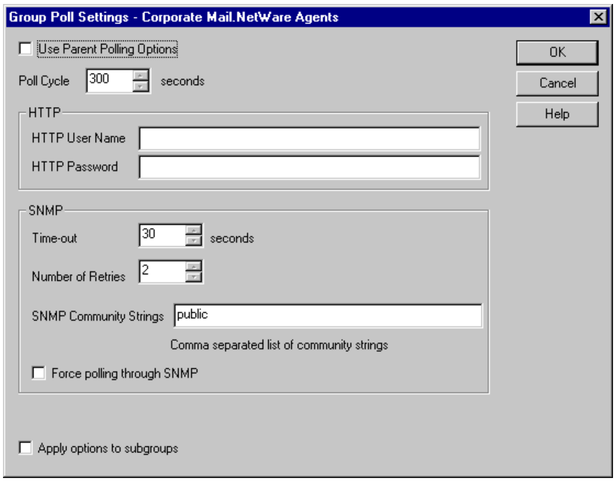
or

Select any agent to set the poll cycle for that individual agent.

2 Click Configuration > Poll Settings.

or

On Linux, click Preferences > Setup, then scroll down to the HTTP Settings section.



Group Poll Settings - Corporate Mail.NetWare Agents

□ Use Parent Polling Options

Poll Cycle: 300 seconds

HTTP

HTTP User Name:

HTTP Password:

SNMP

Time-out: 30 seconds

Number of Retries: 2

SNMP Community Strings: public

Comma separated list of community strings

□ Force polling through SNMP

□ Apply options to subgroups

Unless you selected the root agent group, Use Parent Notification Options is selected and all options are dimmed. Deselect Use Parent Notification Options to set up e-mail notification for an agent group.

3 Increase or decrease the poll cycle as needed, then click OK.

Configuring E-Mail Notification of Agent Problems

The Monitor Agent can notify you by e-mail when agent problems arise.

- "Configuring E-Mail Notification" on page 918
- "Customizing Notification Thresholds" on page 920

Configuring E-Mail Notification

You can configure the Monitor Agent to notify one or more users by e-mail if an agent goes down. You can also receive e-mail confirmation messages showing that the Monitor Agent itself is still running normally.

At the Windows Monitor Agent console:

1 Select the root agent group to set up e-mail notification defaults for all monitored agents.

or

Select any agent group to set up e-mail notification for the agents in the selected group.

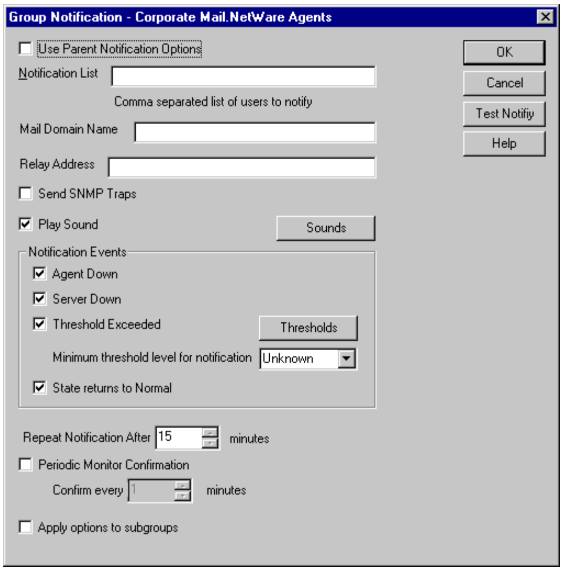
or

Select any agent to set up e-mail notification for that individual agent.

2 Click Configuration > Notification.

or

On Linux, click Preferences > Setup to display the Notify settings.



Group Notification - Corporate Mail.NetWare Agents

□ Use Parent Notification Options

Notification List

Comma separated list of users to notify

Mail Domain Name

Relay Address

□ Send SNMP Traps

☑ Play Sound

Notification Events

☑ Agent Down

☑ Server Down

☑ Threshold Exceeded

Minimum threshold level for notification: Unknown

☑ State returns to Normal

Repeat Notification After 15 minutes

□ Periodic Monitor Confirmation

Confirm every 1 minutes

□ Apply options to subgroups

Unless you selected the root agent group, Use Parent Notification Options is selected and all options are dimmed. Deselect Use Parent Notification Options to set up e-mail notification for an agent group or an individual agent.

3 Specify one or more e-mail addresses or pager addresses to send notifications to.

4 Specify the Internet domain name of your GroupWise system.

5 If the mail system to which e-mail notification is being sent performs reverse DNS lookups, specify the IP address or hostname of a server to relay the notification messages through.

The Monitor Agent should relay e-mail notifications through a server that has a published DNS address.

6 Click Test Notify to determine if the Monitor Agent can successfully send to the addresses specified in the Notification List field.

A message informs you of the results of the test. If the test is successful, a test message arrives shortly at each address. If the test is unsuccessful, double-check the information you provided in the Notification List, Mail Domain Name, and Relay Address fields.

7 Select the events that you want to trigger e-mail notification messages.

- Agent down
- Server down
- Threshold exceeded
- State returns to normal

If you want to be notified of more specific states, see “Customizing Notification Thresholds” on page 920.

8 Select the amount of time that you want to elapse before repeat e-mail notifications are sent.

9. To monitor the Monitor Agent and assure it is functioning normally, select Periodic Monitor Confirmation, select the number of minutes between Monitor Agent e-mail confirmation messages.
10. Click OK to save the e-mail notification settings.

Customizing Notification Thresholds

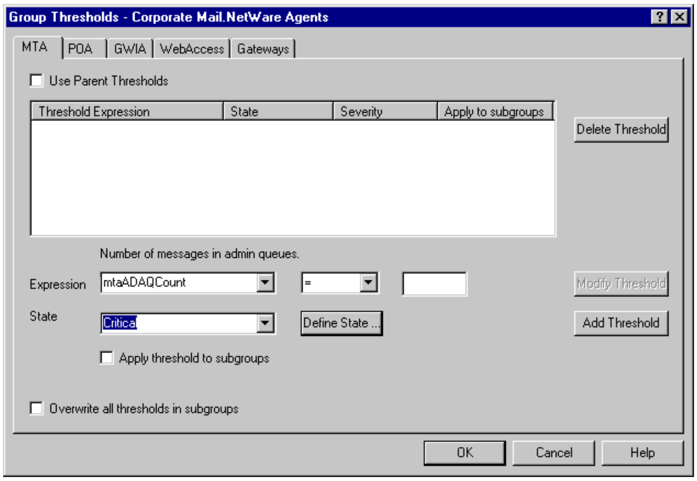
To refine the types of events that trigger e-mail notification messages, you can create your own thresholds that describe very specific states. Using thresholds, you can configure the Monitor Agent to notify you of problem situations peculiar to your GroupWise system.

At the Windows Monitor Agent console:

1. Click Configuration > Notification.
2. Make sure that notification has been properly set up as described in "Configuring E-Mail Notification" on page 918.
3. Click Thresholds.

   or

   On Linux, click Preferences > Thresholds.



Group Thresholds - Corporate Mail.NetWare Agents

□ Use Parent Thresholds

Threshold Expression	State	Severity	Apply to subgroups

Number of messages in admin queues.

Expression: mtaADAQCount =

State: Critical

□ Apply threshold to subgroups

□ Overwrite all thresholds in subgroups

   The tabs at the top of the dialog box enable you to create a separate threshold for each type of GroupWise agent.

4. Select the type of agent to create a threshold for.
5. In the Expression field, select a MIB variable.

   GroupWise agent MIB files are located in the \agents\snmp directory of your GroupWise software distribution directory or *GroupWise 6.5 Administrator* CD. The MIB files list the meanings of the MIB variables and what type of values they represent. The meaning of the MIB variable selected in the Expression field is displayed above the field.

6. Select an operator from the drop-down list.
7. Type the value to test for.
8. In the State field, select an existing state.

Icon	State
?	Unknown
✓	Normal
ℹ	Informational
⚠	Marginal
◆	Warning
⚑	Minor
⚑	Major
⊗	Critical

or

Create a new state:

8a Click Define State

or

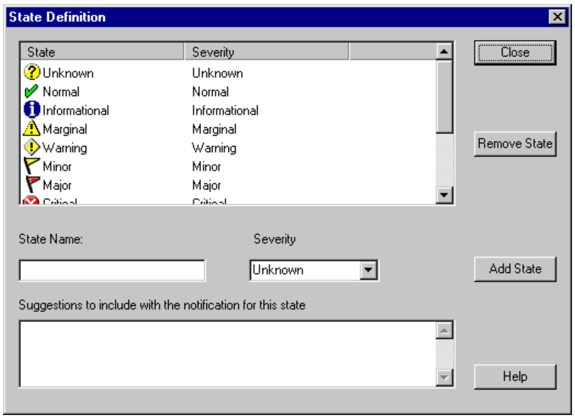
On Linux, click Preferences > States.

8b Type a name for the new state.

8c Select a severity level.

8d Provide instructions about how to handle the new state.

8e Click Close to save the new state.



State	Severity
? Unknown	Unknown
✓ Normal	Normal
ℹ Informational	Informational
⚠ Marginal	Marginal
◆ Warning	Warning
⚑ Minor	Minor
⚑ Major	Major
⊗ Critical	Critical

State Name:

Severity: Unknown

Suggestions to include with the notification for this state

9 Click OK to create the new threshold.

10 Repeat Step 3 through Step 9 for each type of agent that you want to create a customized state for.

11 Make sure Threshold Exceeded is selected in the Notification Events box.

12 Click OK to save the new notification settings.

Configuring Audible Notification of Agent Problems

If the server where the Monitor Agent runs is located where someone can respond immediately to a GroupWise agent problem, you can configure the Monitor Agent to produce a different sound according to the nature of the problem.

NOTE: Audible notification is not available on Linux.

At the Windows Monitor Agent console:

1 Select the root agent group to set up audible notification defaults for all monitored agents.

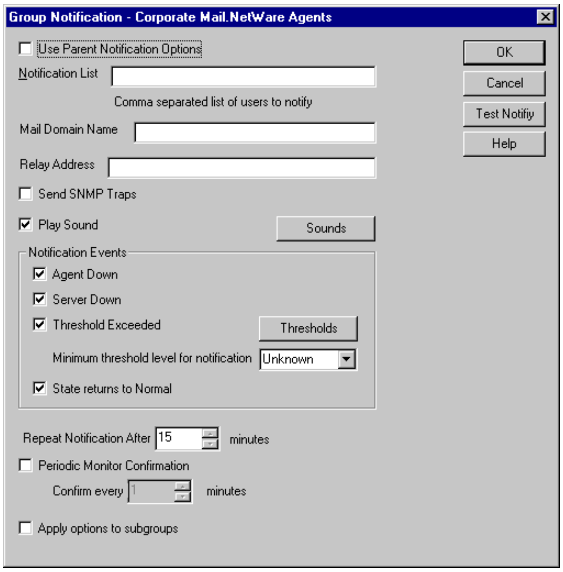
or

Select any agent group to set up audible notification for the agents in the selected group.

or

Select any agent to set up audible notification for that individual agent.

2 Click Configuration > Notification.



Group Notification - Corporate Mail.NetWare Agents

□ Use Parent Notification Options

Notification List

Comma separated list of users to notify

Mail Domain Name

Relay Address

□ Send SNMP Traps

☑ Play Sound

Notification Events

☑ Agent Down

☑ Server Down

☑ Threshold Exceeded

Minimum threshold level for notification: Unknown

☑ State returns to Normal

Repeat Notification After 15 minutes

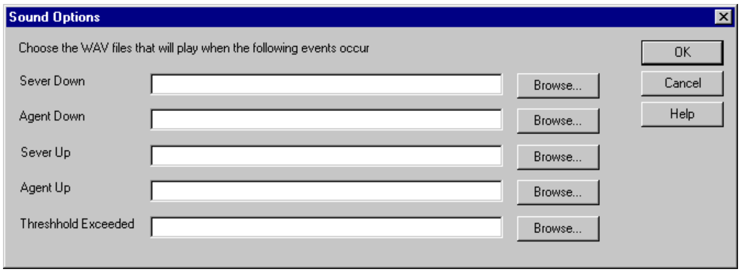
□ Periodic Monitor Confirmation

Confirm every 1 minutes

□ Apply options to subgroups

Unless you selected the root agent group, Use Parent Notification Options is selected and all options are dimmed. Deselect Use Parent Notification Options to set up notification for an agent group or individual agent.

3 Select Play Sound, then click Sounds.



Sound Options

Choose the WAV files that will play when the following events occur

Sever Down

Agent Down

Sever Up

Agent Up

Threshhold Exceeded

4 For each event, browse to and select a sound file to provide auditory notification for each type of event for the selected agent group.

The Monitor Agent launches the default media player for whatever type of sound file you select. Basic sound files are available in the c:\winnt\media directory.

5 Click OK to return to the Notification dialog box.

6 Select notification events and other notification settings as described in "Configuring E-Mail Notification of Agent Problems" on page 918.

7 Click OK to save the audible notification settings.

Configuring SNMP Trap Notification of Agent Problems

The Monitor Agent can throw SNMP traps for use by the Management and Monitoring component of Novell® ZENworks® for Servers, ManageWise®, or any other SNMP management and monitoring program.

At the Windows Monitor Agent console:

1 Select the root agent group to set up SNMP trap notification defaults for all monitored agents.

or

Select any agent group to set up SNMP trap notification for the agents in the selected group.

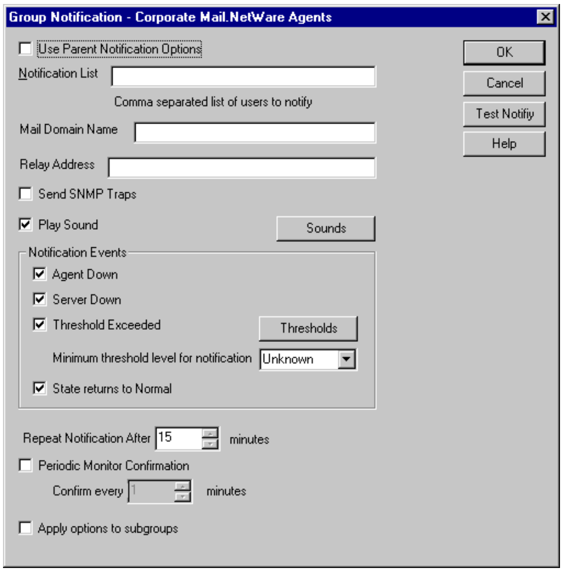
or

Select any agent to set up SNMP trap notification for that individual agent.

2 Click Configuration > Notification.

or

On Linux, click Preferences > Setup to display the Notify settings.



Group Notification - Corporate Mail.NetWare Agents

□ Use Parent Notification Options

Notification List

Comma separated list of users to notify

Mail Domain Name

Relay Address

□ Send SNMP Traps

☑ Play Sound

Notification Events

☑ Agent Down

☑ Server Down

☑ Threshold Exceeded

Minimum threshold level for notification: Unknown

☑ State returns to Normal

Repeat Notification After 15 minutes

□ Periodic Monitor Confirmation

Confirm every 1 minutes

□ Apply options to subgroups

Unless you selected the root agent group, Use Parent Notification Options is selected and all options are dimmed. Deselect Use Parent Notification Options to set up notification for an agent group or individual agent.

3 Select Send SNMP Traps, then click OK.

4 Make sure that the Monitor Agent is properly configured for SNMP, as described in "Configuring the Monitor Agent for SNMP" on page 916.

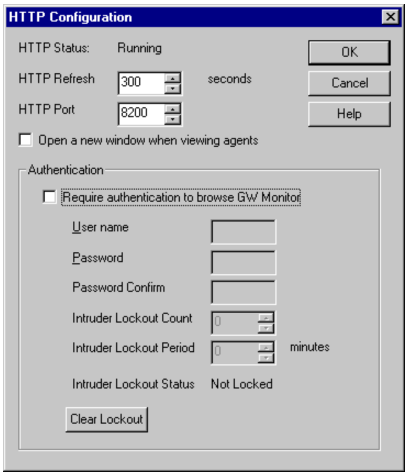
Configuring Authentication and Intruder Lockout for the Monitor Web Console

Accessing GroupWise agent status information from your Web browser is very convenient. However, you might want to limit access to that information. You can configure the Monitor Agent to request a username and password before allowing users to access the Monitor Web console. In addition, you can configure the Monitor Agent to detect break-in attempts in the form of repeated unsuccessful logins.

NOTE: To limit access on Linux, use the --httpmonuser and --httpmonpassword startup switches on the command line when you start the Monitor Agent. The intruder lockout functionality is not available on Linux.

At the Windows Monitor Agent console:

1 Click Configuration > HTTP.



HTTP Configuration

HTTP Status: Running

HTTP Refresh 300 seconds

HTTP Port 8200

□ Open a new window when viewing agents

Authentication

□ Require authentication to browse GW Monitor

User name

Password

Password Confirm

Intruder Lockout Count 0

Intruder Lockout Period 0 minutes

Intruder Lockout Status Not Locked

2 In the Authentication box, select Require Authentication to browse GW Monitor.

3 Fill in the fields:

User Name: Provide a username for the Monitor Agent to prompt for when a user attempts to access the Monitor Web console.

Password: Provide a password for the Monitor Agent to prompt for when a user attempts access. Repeat the password in the Password Confirm field.

To provide additional security for the Monitor Web console, use the /httpssl and /httpcertfile startup switches when starting the Monitor Agent.

Intruder Lockout Count: Specify the number of failed attempts the Monitor Agent should allow before it stops prompting the potentially unauthorized user for a valid username and password.

Intruder Lockout Period: Specify the number of minutes that must elapse before the user can again attempt to access the Monitor Web console.

If a valid user gets locked out of the Monitor Web console, you can use Clear Lockout to grant access before the intruder lockout period has elapsed.

4 Click OK to put the authentication settings into effect.

Configuring Proxy Service Support for the Monitor Web Console

By default, the Monitor Agent and Monitor Web console are not configured to support browser-based access to the Monitor Agent through a firewall. If you require this functionality, you need to enable the Monitor Agent and Monitor Web console to support proxy service.

1 In a text editor, open the Monitor Application configuration file (gwmonitor.cfg)

On Linux, the default location is /opt/novell/groupwise/agents/gwmonitor. On Windows, the default location is c:\novell\gwmonitor

2 Locate the following line:

```
Provider.GWMP.Agent.Http.level=basic
```

3 Change it to:

```
Provider.GWMP.Agent.Http.level=full
```

The BASIC setting restricts use of the Monitor Web console to within a firewall, while the FULL setting allows use of the Web console both inside and outside a firewall. A third setting, NONE, disables use of the Web console.

4 Save and exit the Monitor Application configuration file.

5 Start the Monitor Agent with the /proxy startup switch.

The /proxy switch must be used on the command line or in a script or batch file. The Monitor Agent does not use a startup file for switches.

Without proxy service support enabled, the Monitor Web console, after it gets a GroupWise agent's address from the Monitor Agent, communicates directly with the GroupWise agent. This process, however, does not work when communicating through a firewall.

With proxy service support enabled, all communication is routed through the Monitor Agent and Monitor Application (on the Web server). As long as the Web server can be accessed through the firewall, the Monitor Web console can receive information about all GroupWise agents that the Monitor Agent knows about.

Configuring Monitor Agent Log Settings

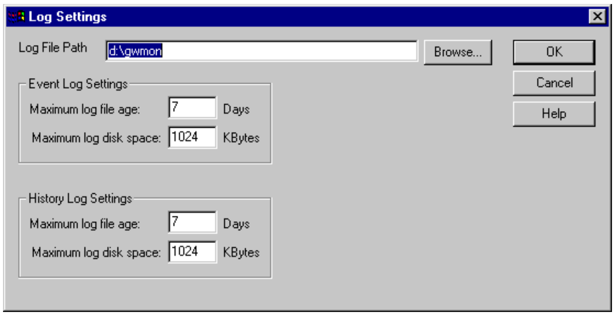
The Monitor Agent writes to two different types of log files. Event log files record error messages, status messages, and other types of event-related messages. History log files record dumps of all MIB values gathered during each poll cycle. Log files can provide a wealth of information for resolving problems with Monitor Agent functioning or agent monitoring.

At the Windows Monitor Agent console:

1 Click Log > Log Settings.

or

On Linux, click Log.



Log File Path: d:\gwmon

Event Log Settings

Maximum log file age: 7 Days

Maximum log disk space: 1024 KBytes

History Log Settings

Maximum log file age: 7 Days

Maximum log disk space: 1024 KBytes

2 Fill in the fields:

Log File Path: Specify the full path of the directory where the Monitor Agent writes its log files. On Linux, the default directory is /var/log/novell/groupwise/gwmon. On Windows, the default is the GroupWise Monitor installation directory (typically c:\gwmon).

Maximum Event Log File Age: Specify the number of days you want Monitor Agent event log files to remain on disk before being automatically deleted. The default event log file age is 7 days.

Maximum Event Log Disk Space: Specify the maximum amount of disk space for all Monitor event log files. When the specified disk space is used, the Monitor Agent overwrites existing Monitor Agent event log files, starting with the oldest. The default is 1024 KB of disk space for all Monitor Agent event log files.

Maximum History Log File Age: Specify the number of days you want Monitor Agent history log files to remain on disk before being automatically deleted. The default history log file age is 7 days.

Maximum History Log Disk Space: Specify the maximum amount of disk space for all Monitor history log files. When the specified disk space is used, the Monitor Agent overwrites existing Monitor Agent history log files, starting with the oldest. The default is 1024 KB of disk space for all Monitor Agent history log files.

3 Click OK to put the new log settings into effect.

4 To view existing event logs, click View > View Log Files.

5 To view existing history log files, click Log > View History Files.

67 Using the Monitor Agent Console

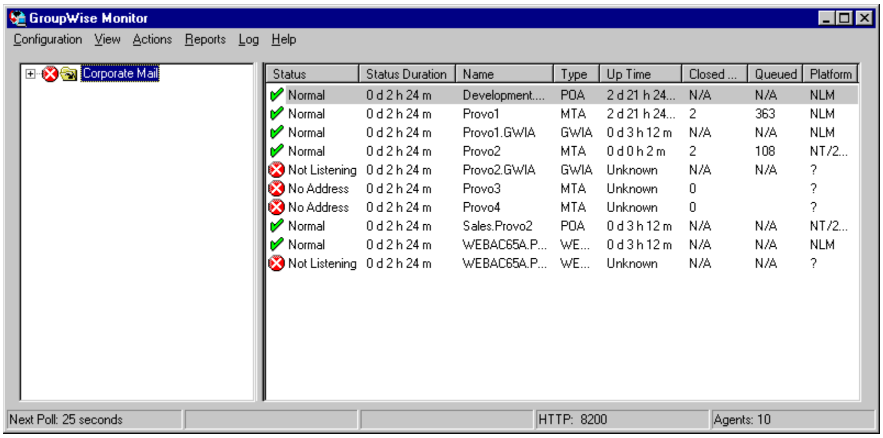
The GroupWise® Windows Monitor Agent console displays GroupWise agent status on the server where the Monitor Agent runs. On Linux, similar information can be displayed in a Web browser.

- "Monitoring Agents at the Monitor Agent Console" on page 927
- "Generating Reports" on page 931
- "Measuring Agent Performance" on page 935

Monitoring Agents at the Monitor Agent Console

Initially, the Monitor Agent console lists all monitored GroupWise agents, along with their statuses.

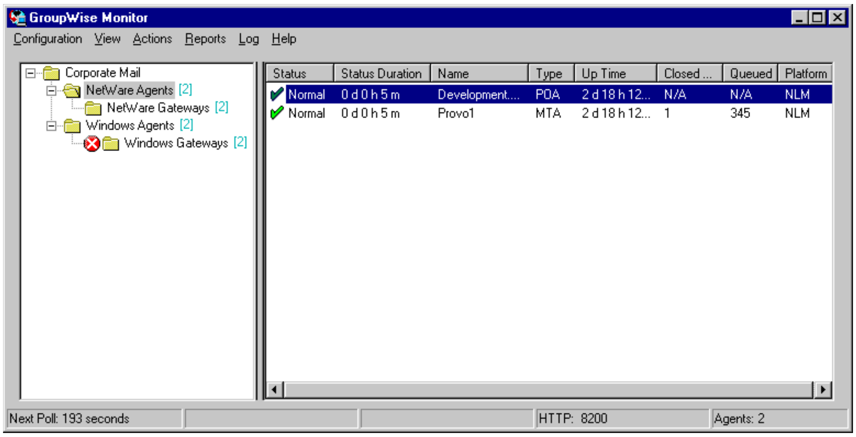
NOTE: On Windows, agents and agent groups are displayed at the Monitor Agent console. On Linux, agents groups are displayed only at the Monitor Web console.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 2 h 24 m	Development....	POA	2 d 21 h 24...	N/A	N/A	NLM
✓ Normal	0 d 2 h 24 m	Provo1	MTA	2 d 21 h 24...	2	363	NLM
✓ Normal	0 d 2 h 24 m	Provo1.GWIA	GWIA	0 d 3 h 12 m	N/A	N/A	NLM
✓ Normal	0 d 2 h 24 m	Provo2	MTA	0 d 0 h 2 m	2	108	NT/2...
☒ Not Listening	0 d 2 h 24 m	Provo2.GWIA	GWIA	Unknown	N/A	N/A	?
☒ No Address	0 d 2 h 24 m	Provo3	MTA	Unknown	0		?
☒ No Address	0 d 2 h 24 m	Provo4	MTA	Unknown	0		?
✓ Normal	0 d 2 h 24 m	Sales.Provo2	POA	0 d 3 h 12 m	N/A	N/A	NT/2...
✓ Normal	0 d 2 h 24 m	WEBAC65A.P...	WE...	0 d 3 h 12 m	N/A	N/A	NLM
☒ Not Listening	0 d 2 h 24 m	WEBAC65A.P...	WE...	Unknown	N/A	N/A	?

Next Poll: 25 seconds | HTTP: 8200 | Agents: 10

After you create agent groups, as described in "Creating and Managing Agent Groups" on page 912, the agents in each group are displayed when you select a group.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 0 h 5 m	Development....	POA	2 d 18 h 12...	N/A	N/A	NLM
✓ Normal	0 d 0 h 5 m	Provo1	MTA	2 d 18 h 12...	1	345	NLM

You can display many types of monitoring information at the Monitor Agent console.

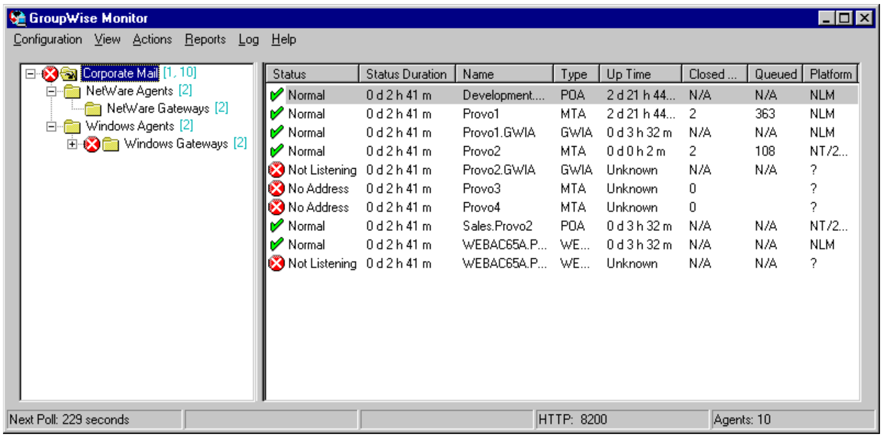
- "Viewing All Agents" on page 928
- "Viewing Problem Agents" on page 928
- "Viewing an Agent Console" on page 929
- "Viewing an Agent Web Console" on page 930
- "Polling the Agents for Updated Status Information" on page 930

Viewing All Agents

After you have separated your agents into groups, you can still view all agents in your GroupWise system in a single list.

At the Windows Monitor Agent console:

1 Right-click the root agent group, then click Show Agent Subgroups.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
✓ Normal	0 d 2 h 41 m	Development....	POA	2 d 21 h 44...	N/A	N/A	NLM
✓ Normal	0 d 2 h 41 m	Provo1	MTA	2 d 21 h 44...	2	363	NLM
✓ Normal	0 d 2 h 41 m	Provo1.GWIA	GWIA	0 d 3 h 32 m	N/A	N/A	NLM
✓ Normal	0 d 2 h 41 m	Provo2	MTA	0 d 0 h 2 m	2	108	NT/2...
☒ Not Listening	0 d 2 h 41 m	Provo2.GWIA	GWIA	Unknown	N/A	N/A	?
☒ No Address	0 d 2 h 41 m	Provo3	MTA	Unknown	0		?
☒ No Address	0 d 2 h 41 m	Provo4	MTA	Unknown	0		?
✓ Normal	0 d 2 h 41 m	Sales.Provo2	POA	0 d 3 h 32 m	N/A	N/A	NT/2...
✓ Normal	0 d 2 h 41 m	WEBAC65A.P...	WE...	0 d 3 h 32 m	N/A	N/A	NLM
☒ Not Listening	0 d 2 h 41 m	WEBAC65A.P...	WE...	Unknown	N/A	N/A	?

You can use the Show Agent Subgroups feature on any group that contains nested subgroups.

Viewing Problem Agents

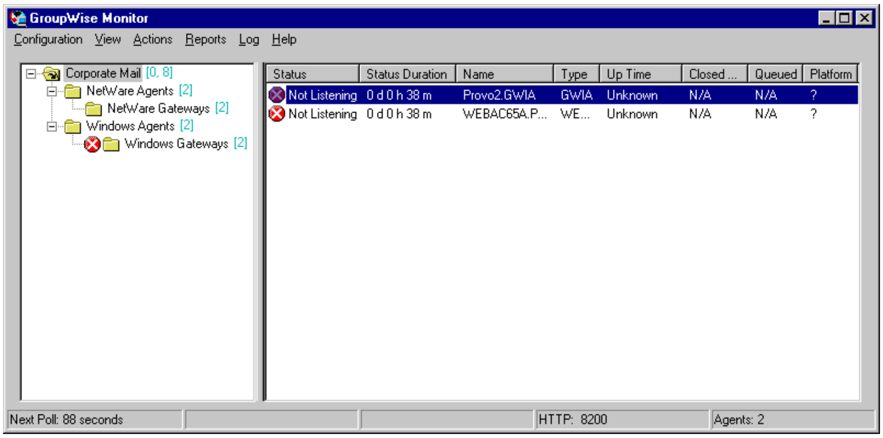
In a single agent group or in a group with subgroups shown, you can filter the list to show only those agents whose status is not Normal.

At the Windows Monitor Agent console:

1 Click View > Problem Agents.

or

On Linux, click Problems.



Status	Status Duration	Name	Type	Up Time	Closed ...	Queued	Platform
Not Listening	0 d 0 h 38 m	Provo2.GWIA	GWIA	Unknown	N/A	N/A	?
Not Listening	0 d 0 h 38 m	WEBAC65A.P...	WE...	Unknown	N/A	N/A	?

Next Poll: 88 seconds | HTTP: 8200 | Agents: 2

Only problem agents are now displayed. If you leave the Monitor Agent with only problem agents displayed, many groups might appear empty because all agents have a status of Normal.

2 To view all monitored agents again, click View > All Agents.

or

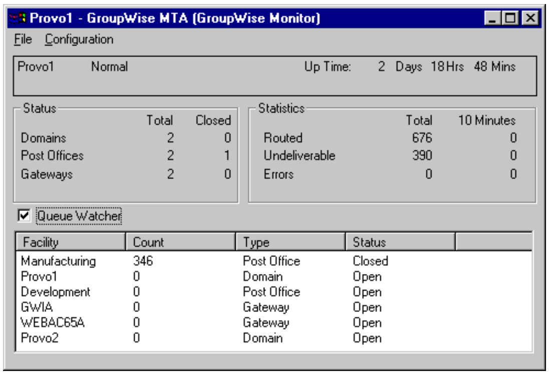
On Linux, click System.

Viewing an Agent Console

An active agent console displays on each server where a GroupWise agent is running. You can display a similar agent console from the Windows Monitor Agent console.

NOTE: This feature is not available on Linux.

1 Right-click an agent, then click Agent Console.



Provo1 Normal Up Time: 2 Days 18Hrs 48 Mins

Status

	Total	Closed
Domains	2	0
Post Offices	2	1
Gateways	2	0

Statistics

	Total	10 Minutes
Routed	676	0
Undeliverable	390	0
Errors	0	0

☑ Queue Watcher

Facility	Count	Type	Status
Manufacturing	346	Post Office	Closed
Provo1	0	Domain	Open
Development	0	Post Office	Open
GWIA	0	Gateway	Open
WEBAC65A	0	Gateway	Open
Provo2	0	Domain	Open

You cannot control the agent from the Monitor Agent like you can at the actual agent console, but you can gather status information about the monitored agent.

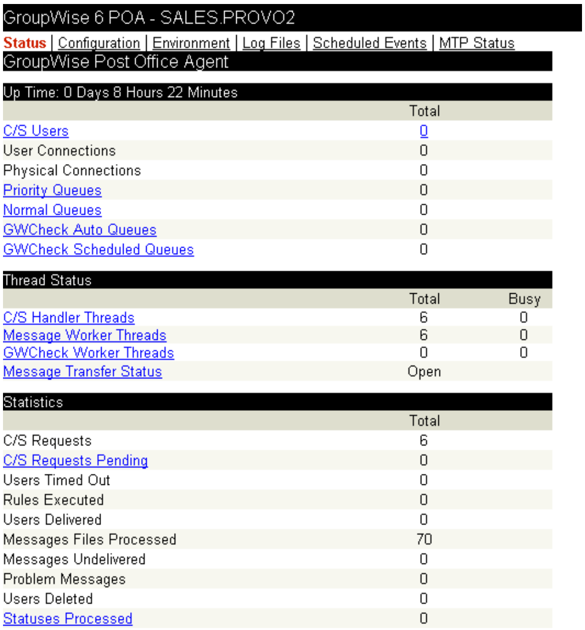
Viewing an Agent Web Console

An agent Web console can be displayed anywhere you have access to a Web browser and the Internet. You can launch an agent Web console from the Windows Monitor Agent console.

1 Right-click an agent, then click Agent Web Console.

or

On Linux, click the domain or post office link.



GroupWise 6 POA - SALES.PROVO2

Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status

GroupWise Post Office Agent

Up Time: 0 Days 8 Hours 22 Minutes	
	Total
C/S Users	0
User Connections	0
Physical Connections	0
Priority Queues	0
Normal Queues	0
GWCheck Auto Queues	0
GWCheck Scheduled Queues	0

Thread Status		
	Total	Busy
C/S Handler Threads	6	0
Message Worker Threads	6	0
GWCheck Worker Threads	0	0
Message Transfer Status	Open	

Statistics	
	Total
C/S Requests	6
C/S Requests Pending	0
Users Timed Out	0
Rules Executed	0
Users Delivered	0
Messages Files Processed	70
Messages Undelivered	0
Problem Messages	0
Users Deleted	0
Statuses Processed	0

For information about the agent Web consoles, see the GroupWise agent documentation:

- "Using the POA Web Console" on page 489
- "Using the MTA Web Console" on page 617
- "Monitoring the Internet Agent through the Web Console" on page 742
- "Monitoring the WebAccess Agent through the Web Console" on page 879

Polling the Agents for Updated Status Information

By default, the Monitor Agent polls the monitored agents every five minutes. You can change the default poll cycle, as described in "Configuring Polling of Monitored Agents" on page 917 The time remaining until the next poll cycle is displayed in the lower left corner of the Monitor Agent console.

You can also manually poll monitored agents:

- To poll all agents, click Action > Poll All Agents.

  or

  On Linux, click Poll.

- To poll a specific agent, right-click the agent, then click Poll Agent.

- To stop polling a specific agent (for example, because the server it runs on is awaiting repairs), right-click the agent, then click Suspend Polling. You can specify a time interval for the agent to be suspended, after which polling resumes automatically. By suspending polling, you prevent repeat notifications for a problem that is already being addressed.

  The suspended agent's status is listed as Suspended, accompanied by the same icon used for the Unknown status ?.

- To restart regular polling of an agent for which polling was suspended, right-click the agent, then click Resume Polling.

Generating Reports

You can generate reports on demand at the Monitor Agent console to help you manage message flow throughout your GroupWise system.

- "Link Trace Report" on page 931
- "Link Configuration Report" on page 932
- "Environment Report" on page 933
- "User Traffic Report" on page 933
- "Link Traffic Report" on page 934
- "Message Tracking Report" on page 934
- "Performance Tracking Report" on page 935

Link Trace Report

A link trace report enables you to follow the path a message would take between two GroupWise domains. A link trace report includes a list of all the domains through which a message would need to pass, along with their current status, link type, address, and number of messages currently queued in each domain. If any domain along the link path is closed, an error message is displayed.

If a message fails to arrive at its destination, this report can help you pinpoint its current location, so you can resolve the problem and get messages flowing smoothly again.

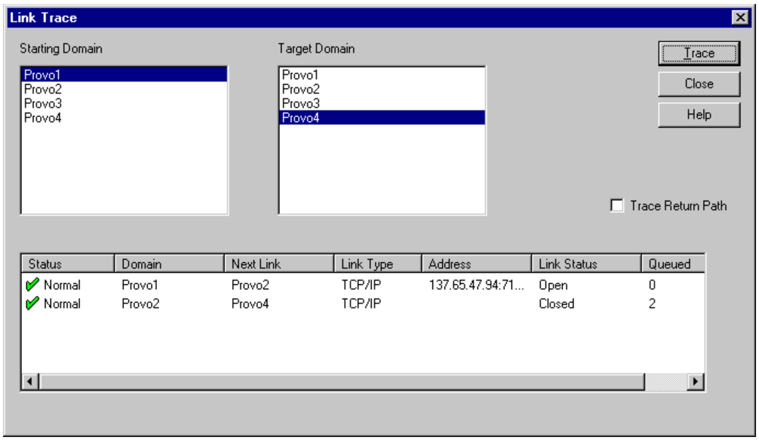
At the Windows Monitor Agent console:

1. Click Reports > Link Trace.

   or

   On Linux, click Link Trace.

2. Select a starting domain and a target domain.
3. If you want to trace the path back, which is the route status messages will take, select Trace Return Path.
4. Click Trace.



Starting Domain

Provo1
Provo2
Provo3
Provo4

Target Domain

Provo1
Provo2
Provo3
Provo4

Status	Domain	Next Link	Link Type	Address	Link Status	Queued
✓ Normal	Provo1	Provo2	TCP/IP	137.65.47.94:71...	Open	0
✓ Normal	Provo2	Provo4	TCP/IP		Closed	2

If any domain in the path is closed, an error message displays so you know where the problem is occurring.

5 When you are finished tracing links, click Close.

Link Configuration Report

A link configuration report enables you to list the links from one or more GroupWise domains to all other domains in your GroupWise system. This helps you identify inefficient link paths, loops, and unreachable domains. All domains must be open to obtain an accurate link map of your GroupWise system.

At the Windows Monitor Agent console:

1 Make sure all domains in your GroupWise system are open.

You cannot obtain an accurate link map of your GroupWise system if any domains are closed. For assistance with closed domains, see "Message Transfer Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

2 Click Reports > Link Configuration

or

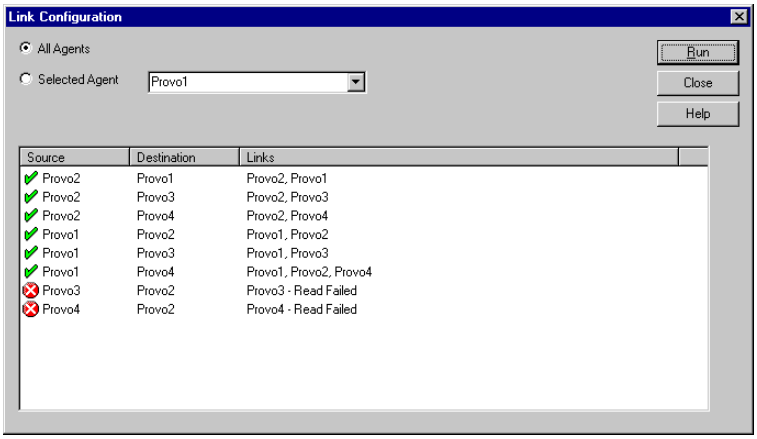
On Linux, click Link Configuration

3 Select All Agents

or

Select a specific agent from the drop-down list.

4 Click Run



● All Agents

○ Selected Agent Provo1

Source	Destination	Links
✓ Provo2	Provo1	Provo2, Provo1
✓ Provo2	Provo3	Provo2, Provo3
✓ Provo2	Provo4	Provo2, Provo4
✓ Provo1	Provo2	Provo1, Provo2
✓ Provo1	Provo3	Provo1, Provo3
✓ Provo1	Provo4	Provo1, Provo2, Provo4
✗ Provo3	Provo2	Provo3 - Read Failed
✗ Provo4	Provo2	Provo4 - Read Failed

The list shows what domains a message would pass through to travel from the domain in the Source column to the domain in the Destination column. If a domain displays as closed, it means that the Monitor Agent could not contact the MTA for the domain or that a loop was detected in the link configuration.

5 When you are finished checking links, click Close.

Environment Report

An environment report lists all monitored agents, along with each agent's location, version, IP address, port number, and operating system information. For NetWare® agents, the server name, CLIB version, TCP/IP version, Novell eDirectory™ version, and the number of packet receive buffers are also listed.

At the Monitor Agent console:

1 Click Reports > Environment.

2 Scroll through the displayed information for your own use.

or

Click Send, type your e-mail address, type one or more e-mail addresses to send the environment report to, then click Send.

3 Click OK to close the Environment Report dialog box.

User Traffic Report

A user traffic report enables you to determine how many messages a user has sent outside his or her post office. The user traffic report lists all messages sent by a specified user during a specified date/time range, along with date, time, and size information for each message. You can also generate a user traffic report for all users whose messages pass through a selected domain.

In order for the information to be available to generate a user traffic report, you must configure the MTA to perform message logging. See "Enabling MTA Message Logging" on page 603.

At the Monitor Agent console:

1 Click Reports > User Traffic.

2 Select the user's domain or the domain you want to generate a user traffic report for.

3 Type the GroupWise user ID that you want to create a report for.

or

Leave the field blank to create a report for all users whose messages pass through the selected domain.

4. If you want to restrict the report to a particular time interval, specify start and end dates and times.
5. Click Run.
6. After the results are displayed, click Save, provide a filename for the report, select the format for the report, then click OK.

   Reports can be saved in comma-separated or tab-separated format to meet the needs of the program you plan to use to display and print the report. For example, you could bring the data into a spreadsheet program. If needed, you can include column headings to create an initial line in the output file that labels the contents of each column.
7. When you are finished generating user traffic reports, click Close.

Link Traffic Report

A link traffic report enables you to determine how many messages are passing from a selected GroupWise domain across a specified link. The link traffic report lists the total number and total size of all messages passing through the link during each hour or half hour of operation.

In order for the information to be available to generate a link traffic report, you must configure the MTA to perform message logging. See "Enabling MTA Message Logging" on page 603.

At the Monitor Agent console:

1. Click Reports > Link Traffic.
2. Select the source domain of the link.

   The list includes all domains that the Monitor Agent uses XML to communicate with. If the Monitor Agent must use SNMP to communicate with a domain, that domain is not included in the list.
3. Select the other end of the link, which could be another domain, a post office, or a gateway.
4. If you want to restrict the report to a particular time interval, specify start and end dates and times.
5. Click Run.
6. After the results are displayed, click Save, provide a file name for the report, select the format for the report, then click OK.

   Reports can be saved in comma-separated or tab-separated format to meet the needs of the program you plan to use to display and print the report. For example, you could bring the data into a spreadsheet program. If needed, you can include column headings to create an initial line in the output file that labels the contents of each column.
7. When you are finished generating link traffic reports, click Close.

Message Tracking Report

A message tracking report enables you to track an individual message through your GroupWise system. The message tracking report provides information about when a message was sent, what queues the message has passed through, and how long it spent in each message queue. If the message has not been delivered, the message tracking report shows where it is.

In order for the information to be available to generate a message tracking report, you must configure the MTAs in your GroupWise system to perform message logging. See "Enabling MTA Message Logging" on page 603.

In addition, you need to determine the message ID of the message. Have the sender check the Sent Item Properties of the message in the GroupWise client. The Mail Envelope Properties field displays the message ID of the message; for example, 3AD5EDEB.31D : 3 : 12763.

At the Monitor Agent console:

1. Click Reports > Message Tracking.
2. Type the message ID of the message to track.

   You can obtain the message file ID in the GroupWise client. Open the Sent Items folder, right-click the message, click Properties, then check the Mail Envelope Properties field for the message file ID; for example, 3A75BAB9.FF1 : 8 : 31642.
3. Select the domain where you want to start tracking.
4. Click Track.
5. When you are finished generating message tracking reports, click Close.

Performance Tracking Report

Before you can run a performance tracking report, you must configuration the Monitor Agent for performance tracking. See "Measuring Agent Performance" on page 935.

Measuring Agent Performance

To test the performance of the agents in your GroupWise system, you can send performance test messages from a specially configured Monitor domain to target domains anywhere in your GroupWise system. The Monitor Agent measures the amount of time it takes for replies to return from the target domains, which lets you ascertain the speed at which messages flow through your GroupWise system.

Perform the following steps to set up agent performance testing:

- "Setting Up an External Monitor Domain" on page 935
- "Selecting an MTA to Communicate with the Monitor Agent" on page 936
- "Configuring the Monitor Agent for Agent Performance Testing" on page 937
- "Viewing Agent Performance Data" on page 938
- "Viewing an Agent Performance Report" on page 938
- "Receiving Notification of Agent Performance Problems" on page 938

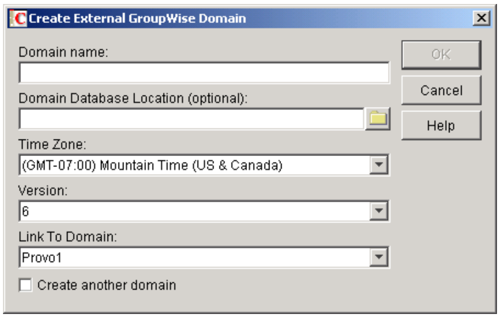
Setting Up an External Monitor Domain

Before you can use the GroupWise Performance Testing dialog box to configure and enable GroupWise performance testing, you must create a specially configured Monitor domain and select an MTA to receive performance test messages from the Monitor Agent. The Monitor Agent uses an external GroupWise domain as part of measuring performance.

In ConsoleOne®:

1 Create an external GroupWise domain.

For information about external GroupWise domains, see "Creating an External Domain" in "Connecting to GroupWise 5.x and 6.x Systems" in the *GroupWise 6.5 Multi-System Administration Guide*. By creating an external domain, you enable the Monitor Agent to approximate the round-trip time for e-mail messages to travel to recipients and for status messages to travel back to senders.



Create External GroupWise Domain

Domain name:

Domain Database Location (optional):

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Version: 6

Link To Domain: Provo1

□ Create another domain

2 Name the external domain to reflect its role in your GroupWise system.

For example, you could name it GW Performance Tester. It does not matter which domain you link the external domain to.

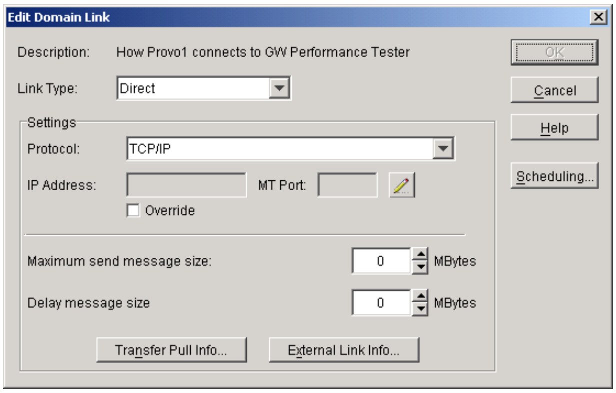
3 Continue with "Selecting an MTA to Communicate with the Monitor Agent" on page 936.

Selecting an MTA to Communicate with the Monitor Agent

The Monitor Agent needs to send its performance testing messages to a specific MTA in your GroupWise system. It does not matter which MTA you decide to use. It could be the MTA for the domain to which the external Monitor domain is linked.

In the Link Configuration Tool in ConsoleOne:

1 Configure the outbound link from the selected MTA to the external Monitor domain to be a TCP/IP link.



Edit Domain Link

Description: How Provo1 connects to GW Performance Tester

Link Type: Direct

Settings

Protocol: TCP/IP

IP Address: MT Port:

□ Override

Maximum send message size: 0 MBytes

Delay message size 0 MBytes

2 Click the pencil icon to provide the IP address of the server where the Monitor Agent runs.

3 Specify a unique port number for the MTA to use to communicate with the Monitor Agent.

Click OK twice to finish modifying the link.

4 Exit the Link Configuration Tool to save the new link configuration information.

5 Continue with "Configuring the Monitor Agent for Agent Performance Testing" on page 937.

Configuring the Monitor Agent for Agent Performance Testing

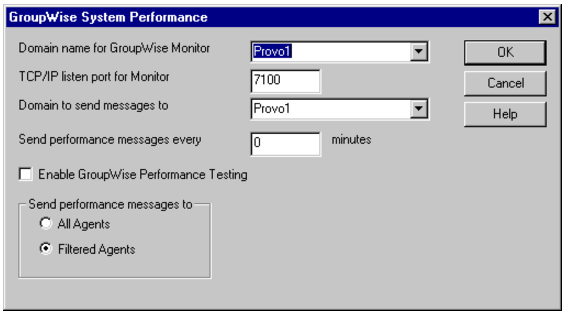
After you have created an external Monitor domain and configured a link from it to an MTA, you are ready to configure the Monitor Agent for performance testing.

At the Windows Monitor Agent console:

1 Click Configuration > Performance Testing.

or

On Linux, click Preferences > Setup, then scroll down to the Performance Testing section.



GroupWise System Performance

Domain name for GroupWise Monitor: Provo1

TCP/IP listen port for Monitor: 7100

Domain to send messages to: Provo1

Send performance messages every 0 minutes

□ Enable GroupWise Performance Testing

Send performance messages to

○ All Agents

● Filtered Agents

2 Fill in the fields:

Domain Name for GroupWise Monitor: Select the external Monitor domain that you configured for system performance testing.

You might need to restart the Monitor Agent in order to see the new Monitor domain in the drop-down list.

TCP/IP Listen Port for Monitor: Specify the port number where you configured the MTA to communicate with the Monitor Agent.

Domain to Send Messages To: Select the domain where the specially configured MTA is running.

The Monitor Agent directs all performance test messages to the selected domain. From there, the MTA transfers the performance test messages to the agents whose performance is being measured.

Send Performance Messages Every: Specify in minutes the time interval for the Monitor Agent to send performance test messages.

Enable GroupWise Performance Testing: Select this option to turn on performance testing. Deselect this option when you have finished your performance testing.

Send Performance Messages To: Select All Agents to send performance test messages to all domains in your GroupWise system. Select Filtered Agents to send performance test messages only to the agents currently listed at the Monitor Agent console.

3 Click OK to put the performance testing settings into effect.

4. Continue with "Viewing Agent Performance Data" on page 938.

   or

   Continue with "Receiving Notification of Agent Performance Problems" on page 938.

Viewing Agent Performance Data

The information gathered by the Monitor Agent through performance test messages is recorded in the Monitor history log.

At the Monitor Agent console:

1. Click Log > View History Files.
2. Select a history log file > click View.

Viewing an Agent Performance Report

A performance testing report enables you to measure how long it takes messages to travel through your GroupWise system. The performance testing report lists each domain that a performance test message was sent to, when it was sent by the Monitor Agent, and the number of seconds between when it was sent and when the Monitor Agent received a response from the tested agent.

At the Monitor Agent Console:

1. Click Reports > Performance Testing.
2. Select All Domains to generate a performance testing report for all domains in your GroupWise system.

   or

   Select one domain to generate a performance testing report for it.
3. Click Run to generate the performance testing report.

Receiving Notification of Agent Performance Problems

If you want the Monitor Agent to notify you if system performance drops to an unacceptable level, you can create a threshold to check the mtaLastResponseTime and mtaAvgResponseTime MIB variables. The average response time is a daily average that is reset at midnight. See "Customizing Notification Thresholds" on page 920 for setup instructions.

Assigning Responsibility for Specific Agents

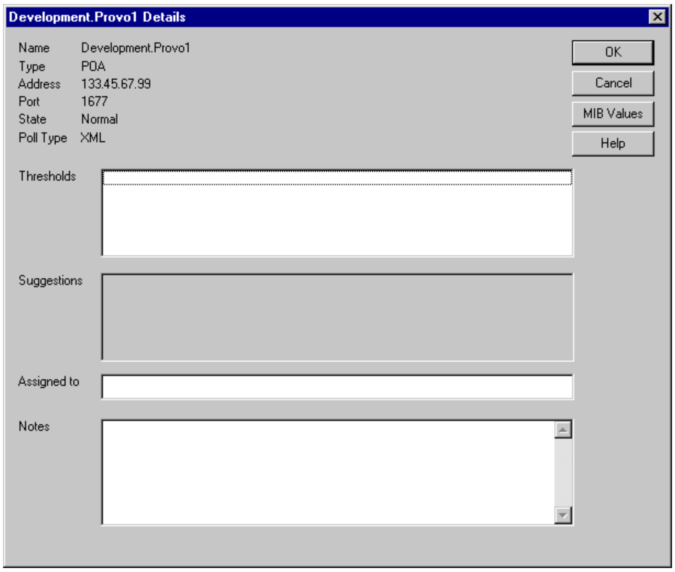
If multiple GroupWise administrators manage the agents throughout your GroupWise system, you can assign a contact for each agent. Or, in a helpdesk environment, a person can be assigned to an agent when a problem occurs. The person assigned to the agent can record notes about the functioning of the agent which are then available to other administrators.

At the Windows Monitor Agent console:

1. Right-click an agent in the agent status window, then click Agent Details.

   or

   On Linux, click the agent status link.



Name Development.Provo1
Type POA
Address 133.45.67.99
Port 1677
State Normal
Poll Type XML

2 In the Assign To field, type the name of the GroupWise administrator who is responsible for this agent.

The name is displayed to the right of the agent status in the status window of the Monitor Agent console and the Monitor Web console.

3 In the Notes box, type any comments you might have about the agent.

If a problem with the agent occurs, the Thresholds box and the Suggestions box displays helpful information about the problem if you have set up customized thresholds, as described in "Customizing Notification Thresholds" on page 920.

4 Click OK to save the information about who is assigned to the agent.

68 Configuring the Monitor Application

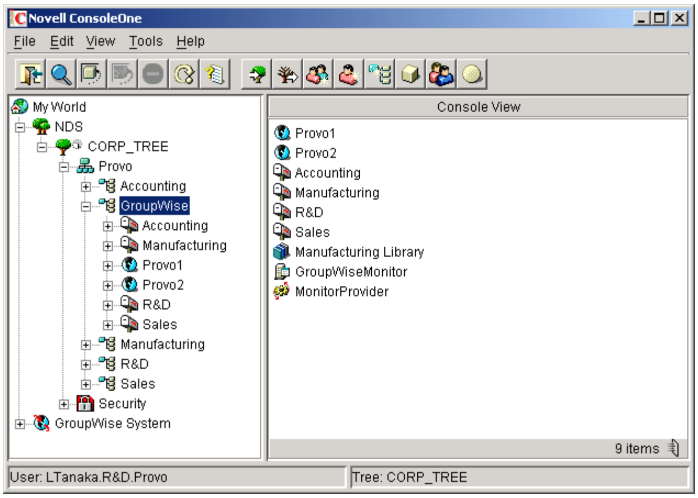
During installation, the GroupWise® Monitor Application is set up with a default configuration. However, you can use the information in the following sections to optimize the Monitor Application configuration:

- "Modifying Monitor Application Environment Settings" on page 941
- "Modifying Monitor Application Log Settings" on page 942
- "Adding or Removing Service Providers" on page 944
- "Modifying Monitor Application Template Settings" on page 945

Modifying Monitor Application Environment Settings

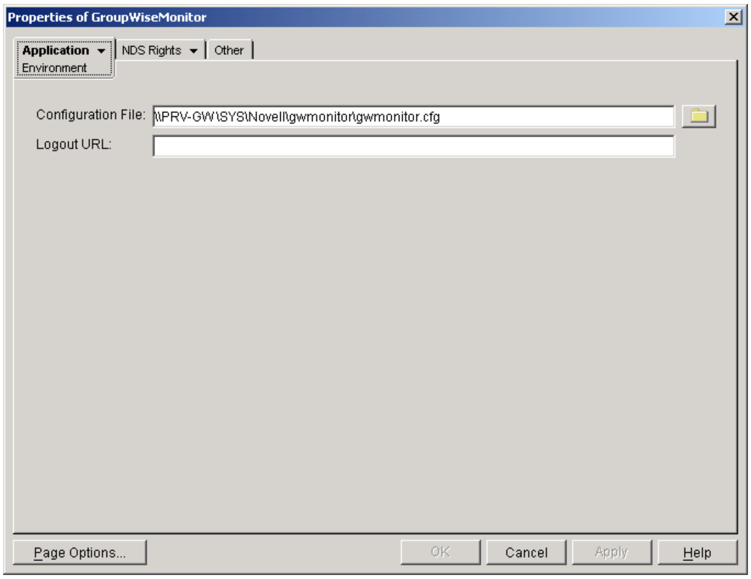
Using ConsoleOne®, you can modify the Monitor Application's environment settings. The environment settings determine such things as the location where ConsoleOne stores the Monitor Application's configuration file and how long the Monitor Application maintains an open session with an inactive user.

1 In ConsoleOne, use the Console View to browse to the Monitor Application object (named GroupWiseMonitor).



The Monitor Application object is not available in the GroupWise View.

2 Right-click the Monitor Application object, then click Properties to display the Environment page.



Configuration File: \\PRV-GW\SYS\Novell\gwmonitor\gwmonitor.cfg

Logout URL:

3 Modify the fields as needed:

Configuration File: The Monitor Application does not have access to Novell® eDirectory® or the GroupWise domain database (wpdomain.db). Therefore, ConsoleOne writes the application's configuration information to the file specified in this field. By default, this is the gwmonitor.cfg file located in the Monitor Application's home directory (novell\gwmonitor at the root of the Web server). On Linux, the gwmonitor.cfg file is located in the /opt/novell/groupwise/gwmonitor directory.

In general, you should avoid changing the location of the file. If you do change the location of the file, you need to make sure to modify the gwmonitor.cfg path in the servlets.properties file, located in the novell\servletgateway\servlets directory on a Windows server or the Java servlet directory on a NetWare® or UNIX server. If you do not, the Monitor Application continues to look for its configuration information in the old location. On Linux, do not change the location of the gwmonitor.cfg file.

Logout URL: By default, if users are required to log in to the Monitor Web console, they are returned to the login page when they log out. If desired, you can enter the URL for a different page.

4 Click OK to save the changes.

Modifying Monitor Application Log Settings

The Monitor Application logs information to log files on disk. You can control the following logging features:

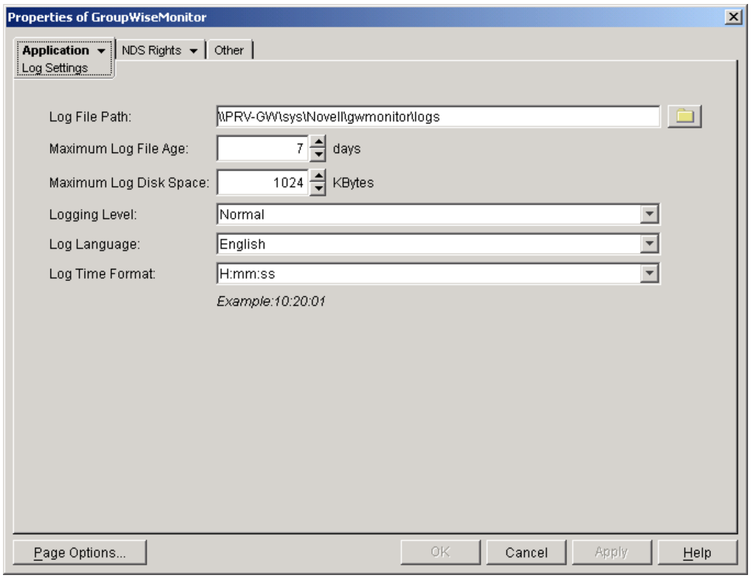
- The type of information to log
- How long to retain log files
- The maximum amount of disk space to use for log files
- Where to store log files

The Monitor Application creates a new log file each day and each time it is restarted (as part of the Web server startup). The log file is named *mmdd*mon.*nnn*, where *mm* is the month, *dd* is the year, and *nnn* is a sequenced log file number (001 for the first log file of the day, 002 for the second, and so forth).

To modify the log settings:

1 In ConsoleOne, browse to and right-click the Monitor Application object (named GroupWiseMonitor), then click Properties.

2 Click Application > Log Settings.



Log File Path: \\PRV-GW\sys\Novell\gwmonitor\logs

Maximum Log File Age: 7 days

Maximum Log Disk Space: 1024 KBytes

Logging Level: Normal

Log Language: English

Log Time Format: H:mm:ss

Example:10:20:01

3 Modify the log settings as needed:

Log File Path: Specify the path to the directory where you want to store the log files.

By default, the log files are stored in the novell\gwmonitor\logs directory at the root of the Web server. On Linux, the log files are stored in the /var/log/novell/groupwise/gwmon directory.

Maximum Log File Age: Specify the number of days you want to retain the log files. The Monitor Application retains the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.

Maximum Log Disk Space: Specify the maximum amount of disk space you want to use for the log files. If the disk space limit is exceeded, the Monitor Application deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 1024 KB.

Logging Level: There are four logging levels: None, Normal, Verbose, and Diagnostic. None turns logging off; Normal displays warnings and errors; Verbose displays Normal logging plus information messages and user requests; and Diagnostic displays all possible information. The default is Normal logging. Use Diagnostic only if you are troubleshooting a problem with Monitor.

The verbose and diagnostic logging levels do not degrade Monitor Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Log Language: Select the language in which you want information written to the log files. The list contains many languages, some of which the Monitor Application might not support. If you select an unsupported language, the information is written in English.

Log Time Format: Choose from the following formats to use when the Monitor Application records dates and times in the log files: *HH:mm:ss:SS*, *MM/dd: H:mm:ss.SS*, or *dd/MM: H:mm:ss.SS*. *H* and *HH* represent hours, *mm* represents minutes, *ss* and *SS* represent seconds, *MM* represents months, and *dd* represents days.

4 Click OK to save the log settings.

Adding or Removing Service Providers

The Monitor Application receives requests from Monitor Web console users and then passes the requests to the appropriate service provider. The service provider fills the requests and returns the required information to the Monitor Application. The Monitor Application merges the information into the appropriate template and displays it to the user.

To function properly, the Monitor Application must know which service providers are available. The Monitor service provider communicates with the Monitor Agent to fill Monitor Web console requests. The Monitor service provider is installed and configured at the same time as the Monitor Application.

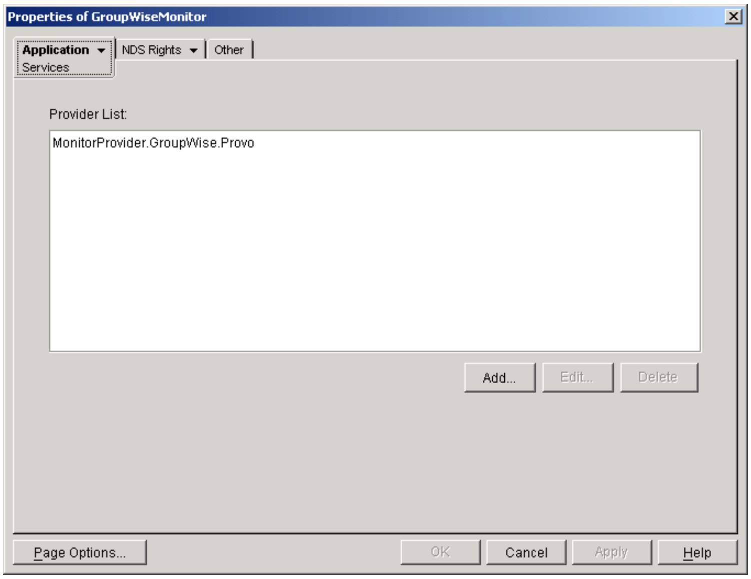
You can disable the Monitor service by removing the Monitor service provider. If you've created new service providers to expose additional services through GroupWise Monitor, you must define those service providers so that the Monitor Application knows about them.

To define service providers:

1 In ConsoleOne, right-click the Monitor Application object (named GroupWiseMonitor), then click Properties.

2 Click Application > Services.

The Provider List displays all service providers that the Monitor Application is configured to use.


Properties of GroupWiseMonitor

Provider List:

MonitorProvider.GroupWise.Provo

3 Choose from the following options:

Add: To add a service provider to the list, click Add, browse to and select the service provider's object, then click OK.

Edit: To edit a service provider's information, select the provider in the list, then click Edit.

Delete: To remove a service provider from the list, select the provider, then click Delete.

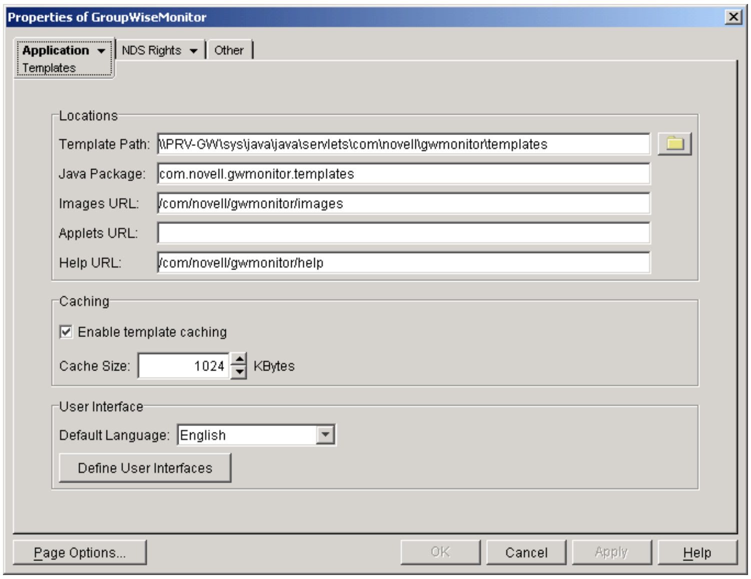
4 Click OK to save the changes.

Modifying Monitor Application Template Settings

When the Monitor Application receives information from a service provider, it merges the information into the appropriate Monitor template before displaying the information to the Monitor Web console user. Using ConsoleOne, you can modify the Monitor Application's template settings. The template settings determine such things as the location of the templates, the maximum amount of server memory to use for caching the templates, and the default template language.

1 In ConsoleOne, browse to and right-click the Monitor Application object (named GroupWiseMonitor), then click Properties.

2 Click Applications > Templates to display the Templates page.



Locations

Template Path: \\PRV-GW\sys\java\java\servlets\com\novell\gwmonitor\templates

Java Package: com.novell.gwmonitor.templates

Images URL: /com/novell/gwmonitor/images

Applets URL:

Help URL: /com/novell/gwmonitor/help

Caching

☑ Enable template caching

Cache Size: 1024 KBytes

User Interface

Default Language: English

3 Modify the fields as needed:

Template Path: Select the location of the template base directory. The template base directory contains the subdirectories (simple, frames, hdml, and wml) for each of the templates provided with GroupWise Monitor. If you create your own templates, you need to place the templates in a new subdirectory in the template base directory.

On a NetWare® server with the Novell Servlet Gateway, the default installation directory is java\servlets\com\novell\gwmonitor\templates.

On a Windows server with the Novell Servlet Gateway, the default installation directory is novell\java\servlets\com\novell\gwmonitor\templates.

On a NetWare or Windows server with Tomcat, the default installation directory is *tomcat_dir*\webapps\ROOT\web-inf\classes\com\novell\gwmonitor\templates.

On a Linux server with Tomcat, the default installation directory is /var/opt/novell/tomcat/webapps/gw/WEB-INF/classes/com/novell/gwmonitor/templates.

Java Package: Specify the Java package that contains the template resources used by the Monitor Application. The default package is com.novell.gwmonitor.templates.

Images URL: Specify the URL for the GroupWise Monitor image files. These images are merged into the templates along with the GroupWise information. This URL must be relative to the Web server's document root directory. On NetWare and Windows, the default relative URL is com\novell\gwmonitor\images. On Linux, the default relative URL is /gw/com/novell/gwmonitor/images.

Applets URL: The Monitor Application does not currently use applets.

Help URL: Specify the URL for the GroupWise Monitor Help files. The default installation directory is the com\novell\gwmonitor\help directory under the Web server's document root directory.

Enable Template Caching: To speed up access to the template files, the Monitor Application can cache the files in memory. Select this option to turn on template caching.

Cache Size: Select the maximum amount of memory, in kilobytes, you want to use when caching the templates. The default cache size, 1024 KB, is sufficient to cache all templates shipped with GroupWise Monitor. If you modify or add templates, you can turn on Verbose logging on the Monitor Application object Log Settings page to view the size of the template files. Using this information, you can then change the cache size appropriately.

Default Language: Select the language to use when displaying the initial Monitor Web console page.

Define User Interfaces: GroupWise Monitor supports Web browsers on many different devices (for example, computers and wireless telephones). Each device supports specific content types such as HTML, HDML, and WML. When returning information to a device's Web browser, the Monitor Application must merge the information into a set of templates to create an interface that supports the content type required by the Web browser.

GroupWise Monitor ships with several predefined user interfaces. These interfaces support Web browsers that require HTML, HDML, and WML content types. Click the User Interface button to view, add, modify, or delete user interfaces.

4 Click OK to save the new template settings.

69 Using the Monitor Web Console

The Monitor Web console displays GroupWise® agent status anywhere a browser and a connection to the Internet are available.

- "Displaying the Monitor Web Console" on page 947
- "Monitoring Agents at the Monitor Web Console" on page 947
- "Managing Links" on page 950
- "Searching for Agents" on page 951

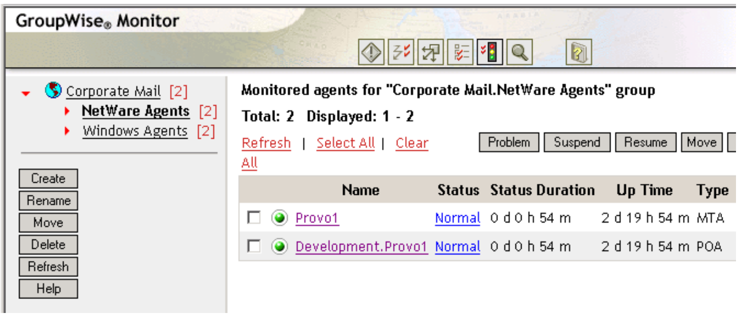
Displaying the Monitor Web Console

1 Make sure that your Web server is running.

2 To display the Monitor Web console, enter the Monitor URL in your Web browser:

Linux: http://*network_address*/gwmon/gwmonitor
Windows: https://*network_address*/servlet/gwmonitor

where *network_address* represents the IP address or hostname of the server where the Monitor Agent is running.



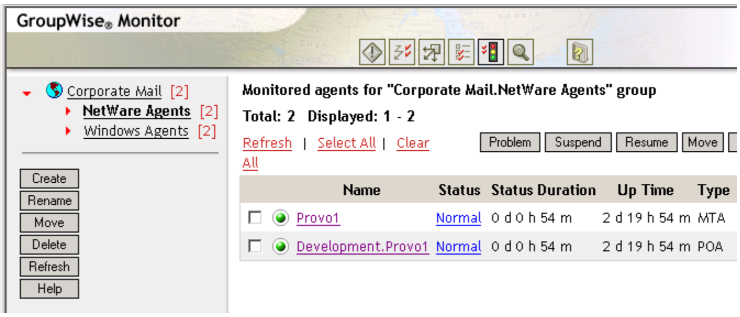
Monitored agents for "Corporate Mail.NetWare Agents" group

Total: 2 Displayed: 1 - 2

	Name	Status	Status Duration	Up Time	Type
□ ●	Provo1	Normal	0 d 0 h 54 m	2 d 19 h 54 m	MTA
□ ●	Development.Provo1	Normal	0 d 0 h 54 m	2 d 19 h 54 m	POA

Monitoring Agents at the Monitor Web Console

The Monitor Web console lists all GroupWise agents that the Monitor agent is polling for status information.



Monitored agents for "Corporate Mail.NetWare Agents" group

Total: 2 Displayed: 1 - 2

	Name	Status	Status Duration	Up Time	Type
□ ●	Provo1	Normal	0 d 0 h 54 m	2 d 19 h 54 m	MTA
□ ●	Development.Provo1	Normal	0 d 0 h 54 m	2 d 19 h 54 m	POA

Features of the Monitor Web console are available on buttons at the top of the Monitor page.

Button	Feature
⚠	Problems
⚡	Link Trace
⇄	Link Configuration
☑	Global Options
🚦	States
🔍	Search

Click an agent group to display all monitored agents in the group. Click the Problem button to display only those agents whose status is other than Normal in the agent group. Click the Problems icon to display all agents in your GroupWise system whose status is other than Normal.

Click the status of an agent to display agent status details.

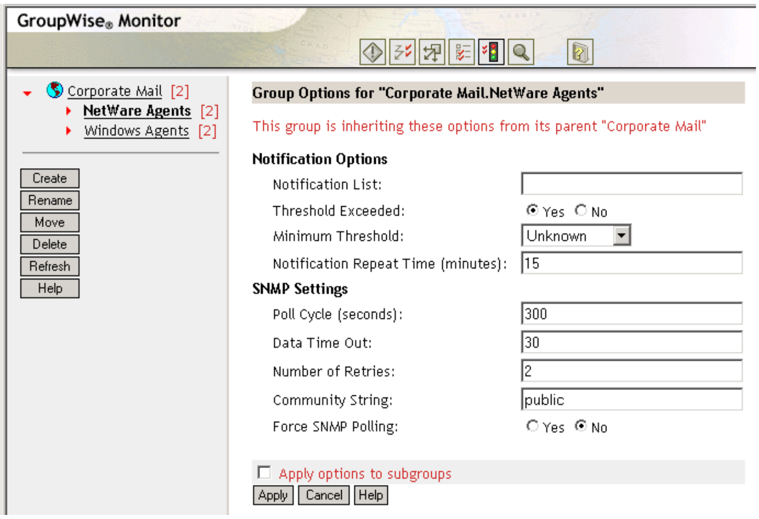
Click an agent in the list to open its agent Web console. For information about the agent Web consoles, see "Viewing an Agent Web Console" on page 930.

Click Refresh to update the agent status information. To modify the default poll cycle, see "Configuring Polling of Monitored Agents" on page 917.

Changing Monitor Agent Configuration Settings at the Monitor Web Console

Some Monitor Agent configuration settings can be changed at the Monitor Web console.

1 To change settings that apply to a particular agent group, click the agent group, then click Options.



Group Options for "Corporate Mail.NetWare Agents"

This group is inheriting these options from its parent "Corporate Mail"

Notification Options

Notification List:	
Threshold Exceeded:	● Yes ○ No
Minimum Threshold:	Unknown
Notification Repeat Time (minutes):	15

SNMP Settings

Poll Cycle (seconds):	300
Data Time Out:	30
Number of Retries:	2
Community String:	public
Force SNMP Polling:	○ Yes ● No

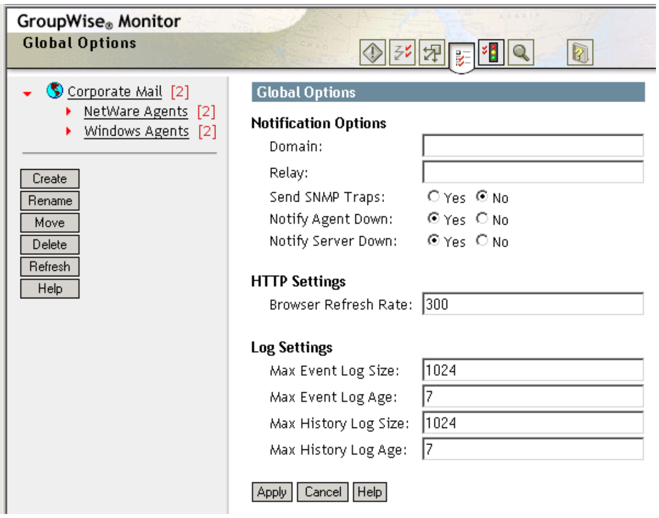
□ Apply options to subgroups

2 Set the options as needed, then click Apply.

For information about the options, see the following sections that describe this functionality for the Windows Monitor Agent console:

- "Configuring E-Mail Notification of Agent Problems" on page 918
- "Configuring Polling of Monitored Agents" on page 917
- "Configuring the Monitor Agent for SNMP" on page 916

3 To change settings that apply to the Monitor Agent itself, rather than to a group of monitored agents, click the Global Options icon.



Global Options

Notification Options

Domain:	
Relay:	
Send SNMP Traps:	○ Yes ● No
Notify Agent Down:	● Yes ○ No
Notify Server Down:	● Yes ○ No

HTTP Settings

Browser Refresh Rate:	300

Log Settings

Max Event Log Size:	1024
Max Event Log Age:	7
Max History Log Size:	1024
Max History Log Age:	7

4 Set the global options as needed, then click Apply.

For information about the options, see the following sections that describe this functionality for the Windows Monitor Agent console:

- "Configuring E-Mail Notification of Agent Problems" on page 918
- "Configuring SNMP Trap Notification of Agent Problems" on page 923
- "Configuring the Monitor Agent for HTTP" on page 915
- "Configuring Monitor Agent Log Settings" on page 925

Managing Links

The Monitor Web console can help you manage links throughout your GroupWise system.

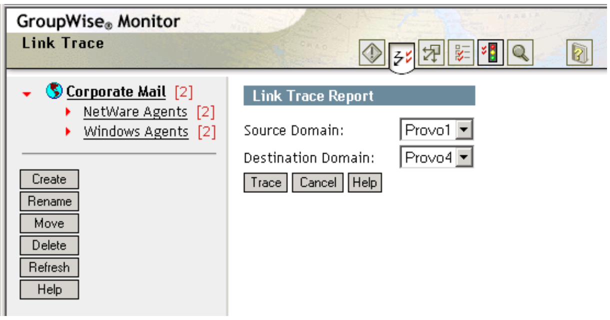
- "Tracing a Link at the Monitor Web Console" on page 950
- "Checking Links Configuration at the Monitor Web Console" on page 950

Tracing a Link at the Monitor Web Console

When you trace a link, you follow the path a message would take when travelling between two GroupWise domains. If a message fails to arrive at its destination, this feature helps you pinpoint its current location, so you can resolve the problem and get messages flowing again.

At the Monitor Web console:

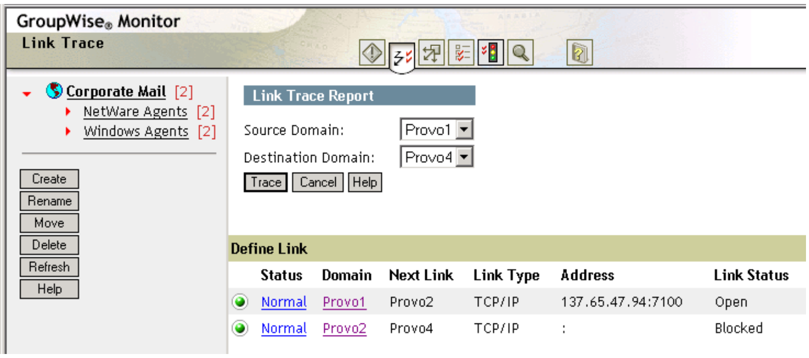
1 Click the Link Trace icon.



Source Domain: Provo1

Destination Domain: Provo4

2 Select a source domain, select a destination domain, then click Trace.



Source Domain: Provo1

Destination Domain: Provo4

Define Link

Status	Domain	Next Link	Link Type	Address	Link Status
● Normal	Provo1	Provo2	TCP/IP	137.65.47.94:7100	Open
● Normal	Provo2	Provo4	TCP/IP	:	Blocked

If any domain in the path is closed, the link trace shows where the problem is occurring.

Checking Links Configuration at the Monitor Web Console

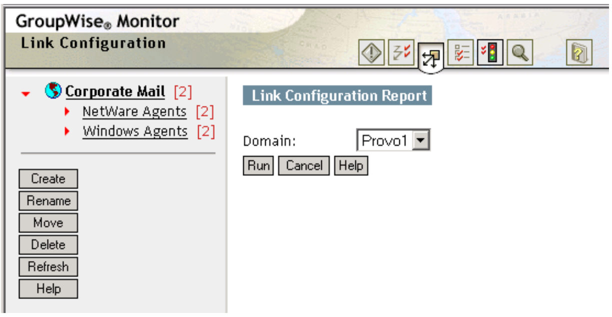
When you check link configuration, you list the links from a GroupWise domain to all other domains in your GroupWise system. This helps you identify inefficient link paths, loops, and unreachable domains.

At the Monitor Web console:

1 Make sure all domains in your GroupWise system are open.

You cannot obtain an accurate link map of your GroupWise system if any domains are closed. For assistance with closed domains, see "Message Transfer Agent Problems" in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

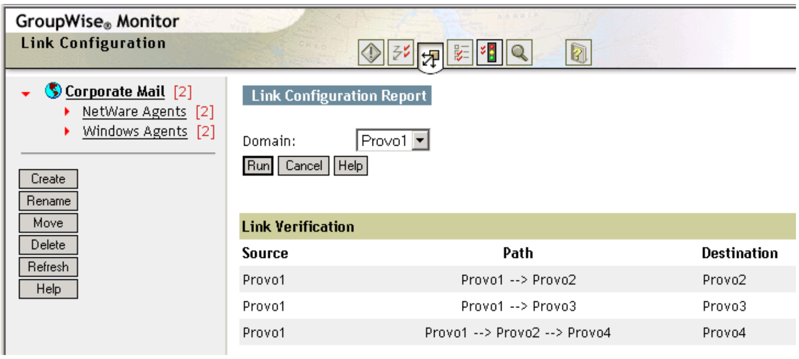
2 Click the Link Configuration icon.



Domain: Provo1

3 Select a domain from the drop-down list.

4 Click Run.



Domain: Provo1

Link Verification

Source	Path	Destination
Provo1	Provo1 --> Provo2	Provo2
Provo1	Provo1 --> Provo3	Provo3
Provo1	Provo1 --> Provo2 --> Provo4	Provo4

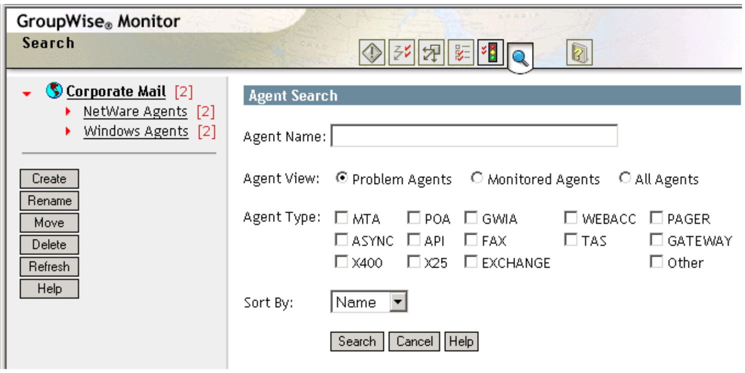
The list shows what domains a message would pass through to travel from the domain in the Source column to the domain in the Destination column.

Searching for Agents

If you monitor a large number of agents, the list displayed in the Monitor Web console can become very long. You can easily search for an individual agent or for a group of related agents.

At the Monitor Web console:

1 Click the Search icon.



Agent Search

Agent Name:

Agent View: ● Problem Agents ○ Monitored Agents ○ All Agents

Agent Type: □ MTA □ POA □ GWIA □ WEBACC □ PAGER □ ASYNC □ API □ FAX □ TAS □ GATEWAY □ X400 □ X25 □ EXCHANGE □ Other

Sort By: Name

2 Type the name of an agent.

or

Select Problems to list all agents whose status is other than Normal.

or

Select one or more types of agent to list.

3 Select the number of instances you want listed at one time.

4 Click Search.

The results display on the Search page with the same functionality as is available on the regular Monitor Web console pages.

70 Comparing the Monitor Agent Consoles

Many aspects of agent monitoring are available in one or more of the Monitor Agent consoles. The table below summarizes agent monitoring features and where they are available.

Task	Windows Monitor Agent Console	Monitor Agent Web Console	Monitor Web Console
Selecting Agents to Monitor	Yes	Yes	No
Creating and Managing Agent Groups	Yes	No	Yes
Viewing All Agents	Yes	Yes	Yes if not in groups
Viewing Problem Agents	Yes	Yes	Yes
Viewing an Agent Console	Yes	No	No
Viewing an Agent Web Console	Yes	Yes	Yes
Searching for Agents	No	No	Yes
Assigning Responsibility for Specific Agents	Yes	Yes	Yes
Configuring the Monitor Agent for HTTP	Yes	Yes	Yes
Configuring the Monitor Agent for SNMP	Yes	Yes	Yes
Configuring Polling of Monitored Agents	Yes	Yes	Yes
Configuring E-Mail Notification of Agent Problems	Yes	Yes	Yes
Configuring Audible Notification of Agent Problems	Yes	No	No
Configuring SNMP Trap Notification of Agent Problems	Yes	Yes	Yes
Configuring Authentication and Intruder Lockout for the Monitor Web Console	Yes	Authentication: Yes Intruder Lockout: No	No
Configuring Monitor Agent Log Settings	Yes	Yes	Yes
Generating Reports	Yes	Yes	Yes
Link Trace Report	Yes	Yes	Yes
Link Configuration Report	Yes	Yes	Yes

Environment Report	Yes	Yes	No
User Traffic Report	Yes	Yes	No
Link Traffic Report	Yes	Yes	No
Message Tracking Report	Yes	Yes	No
Performance Tracking Report	Yes	Yes	No

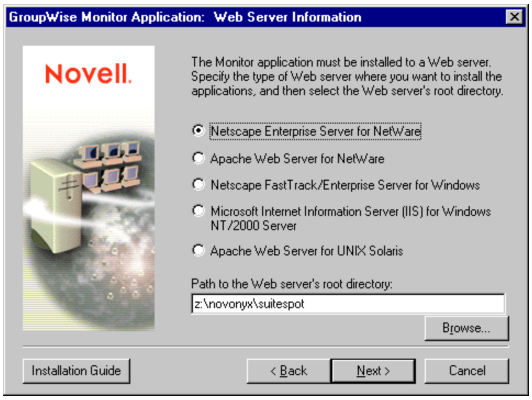
71 Creating a PQA File for the Monitor Web Console

You can use the GroupWise® Monitor Installation program on Windows to create a Web Clipping Application (PQA), also referred to as a Palm Query Application, to enable Palm OS device users to log in to the Monitor Web console.

The Web Clipping Application, named gwmon.pqa, includes the URL required to connect to your GroupWise Monitor installation, a Login page, an About Novell GroupWise page, and the images used when displaying the Monitor Web console on the Palm OS device.

To create a gwmon.pqa file:

1. If you've already created another gwmon.pqa file that you want to keep, make sure it is not in the Web server's *doc_root_directory*\com\novell\gwmonitor\palm\en directory. The Installation program overwrites any gwmon.pqa file in the directory.
2. At a Windows workstation, run setup.exe /pqa from the \admin\monitor directory on the *GroupWise 6.5 Administrator* CD or the GroupWise software distribution directory
3. Select the language for the Installation program, then accept the License Agreement to display the following dialog box.

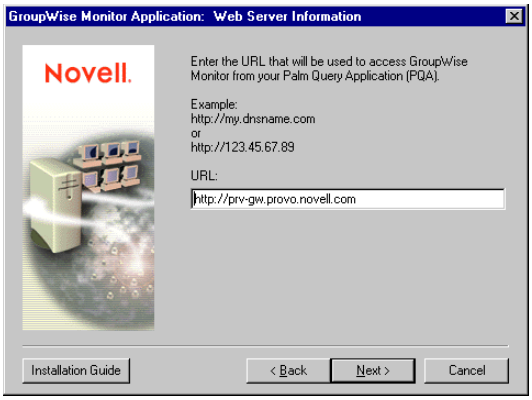


The Monitor application must be installed to a Web server. Specify the type of Web server where you want to install the applications, and then select the Web server's root directory.

● Netscape Enterprise Server for NetWare
○ Apache Web Server for NetWare
○ Netscape FastTrack/Enterprise Server for Windows
○ Microsoft Internet Information Server (IIS) for Windows NT/2000 Server
○ Apache Web Server for UNIX Solaris

Path to the Web server's root directory: z:\novonyx\suitespot

4. Select the type of Web server where the Monitor Web console is installed, make sure the path to the Web server's root directory is correct, then click Next.



Enter the URL that will be used to access GroupWise Monitor from your Palm Query Application (PQA).

Example:
http://my.dnsname.com
or
http://123.45.67.89

URL: http://prv-gw.provo.novell.com

5 Specify the URL you want included in the .pqa file. For example:

```
http://groupwise.novell.com
```

The Installation program automatically appends /servlet/gwmon to the URL so that users are directed to the Monitor Web console login page. For example, using the URL above, the Installation program would create the following URL in the gwmon.pqa file:

```
http://gwroupwise.novell.com/servlet/gwmon
```

As you determine the URL, keep in mind the following:

- If the Web server uses SSL, you should change http to https.
- If you are using a proxy server, you need to enter the proxy server's address.
- The Web clipping proxy server (gateway) does not currently support challenge and response authentication. Therefore, you need to ensure that the Web server is not configured to require basic challenge and response authentication, or at least is configured not to require this authentication for the URL defined in the gwmon.pqa file.

6 Click Next to create the .pqa file, then click Finish.

The gwmon.pqa file is created in the Web server's *doc_root_directory*\com\novell\gwmonitor\palm\en directory. You can distribute it to your Palm OS device users just as you would any other .pqa file.

72 Using Monitor Agent Switches

GroupWise® Monitor Agent startup switches must be used on the command line when you start the Monitor Agent, or in a script or batch file created to start the Monitor Agent. The Monitor Agent does not have a startup file for switches.

Linux Monitor Agent	Windows Monitor Agent
--help	/help
--home	/home
--httpagentpassword	/httpagentpassword
--httpagentuser	/httpagentuser
--httpcertfile	/httpcertfile
--httpmonpassword	/httpmonpassword
--httpmonuser	/httpmonuser
--httpport	/httpport
--httpssl	/httpssl
--ipa	/ipa
--ipp	/ipp
--lang	/lang
--log	/log
--pollthreads	/pollthreads
--proxy	/proxy

/help

Displays the Monitor Agent startup switch Help information. When this switch is used, the Monitor Agent does not start.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--help	/help

/home

Specifies a domain directory, where the Monitor Agent can access a domain database (wpdomain.db). From the domain database, the Monitor Agent can determine which agents to monitor, what usernames and passwords are necessary to access them, and so on.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--home /*directory*	/home-[*svr*\][*vol*:]*dir* /home-\\*svr**vol**dir* /home-[*drive*:]*dir* /home-\\*svr**sharename**dir*
Example:	--home /gwsystem/provo2	/home-\provo2 /home-mail:\provo2 /home-server2\mail:\provo2 /home-\\server2\mail\provo2 /home-\provo2 /home-m:\provo2 /home-\\server2\c\mail\provo2

See also /ipa and /ipp.

/httpagentpassword

Specifies the password for the Monitor Web console to prompt for before allowing GroupWise agent status information to be displayed in your Web browser. Do not use an existing Novell eDirectory password because the information passes over the insecure connection between your Web browser and the Monitor Agent. See "Configuring Authentication and Intruder Lockout for the Monitor Web Console" on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpagentpassword *unique_password*	/httpagentpassword-*unique_password*
Example:	--httpagentpassword AgentWatch	/httpagentpassword-AgentWatch

See also /httpagentuser.

/httpagentuser

Specifies the username for the Monitor Web console to prompt for before allowing GroupWise agent status information to be displayed in your Web browser. Providing a username is optional. Do not use an existing eDirectory username because the information passes over the insecure connection between your Web browser and the Monitor Agent. See "Configuring Authentication and Intruder Lockout for the Monitor Web Console" on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpagentuser *unique_username*	/httpagentuser-*unique_username*
Example:	--httpagentuser MonWebConsole	/httpagentuser-MonWebConsole

See also /httpagentpassword.

/httpcertfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the Monitor Agent and the Monitor Web console displayed in your Web browser. See "Configuring Authentication and Intruder Lockout for the Monitor Web Console" on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpcertfile /*dir*/*file*	/httpcertfile-[*drive*:]\dir\file /httpcertfile-\\svr\sharename\dir\file
Example:	--httpcertfile /certs/gw.crt	/httpcertfile-\ssl\gw.crt /httpcertfile-m:\ssl\gw.crt /httpcertfile-\\\\server2\c\ssl\gw.crt

See also /httpssl.

/httpmonpassword

Specifies the password for the Monitor Web console to prompt for before allowing a user to display the Monitor Web console. Do not use an existing Novell® eDirectory™ password because the information passes over the insecure connection between your Web browser and the Monitor Agent. See "Configuring Authentication and Intruder Lockout for the Monitor Web Console" on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpmonpassword *unique_password*	/httpmonpassword-*unique_password*
Example:	--httpmonpassword WatchIt	/httpmonpassword-WatchIt

See also /httpmonuser.

/httpmonuser

Specifies the username for the Monitor Web console to prompt for before allowing a user to display the Monitor Web console. Providing a username is optional. Do not use an existing eDirectory username because the information passes over the insecure connection between your

Web browser and the Monitor Agent. See "Configuring Authentication and Intruder Lockout for the Monitor Web Console" on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpmonuser *unique_username*	/httpmonuser-*unique_username*
Example:	--httpmonuser MonAdmin	/httpmonuser-MonAdmin

See also /httpmonpassword.

/httpport

Sets the HTTP port number used for the Monitor Agent to communicate with your Web browser. The default is 8200; the setting must be unique. See "Configuring the Monitor Agent for HTTP" on page 915.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpport *port_number*	/httpport-*port_number*
Example:	--httpport 8201	/httpport-9200

/httpssl

Sets the availability of secure SSL communication between the Monitor Agent and the Monitor Web console displayed in your Web browser. Valid values are enabled and disabled. See "Configuring Authentication and Intruder Lockout for the Monitor Web Console" on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpssl *setting*	/httpssl-*setting*
Example:	--httpssl enabled	/httpssl-enabled

See also /httpcertfile.

/ipa

Specifies the network address (IP address or DNS hostname) of a server where an MTA is running. The Monitor Agent can communicate with the MTA to obtain information about agents to monitor.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--ipa *network_address*	/ipa-*network_address*

	Linux Monitor Agent	Windows Monitor Agent
Example:	--ipa 172.16.5.19 --ipa server2	/ipa-172.16.5.20 /ipa-server3

See also /ipp.

/ipp

Specifies the TCP port number associated with the network address of an MTA with which the Monitor Agent can communicate to obtain information about agents to monitor. Typically, the MTA listens for service requests on port 7100.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--ipp *port_number*	/ipp-*port_number*
Example:	--ipp 7110	/ipp-7111

See also /ipa.

/lang

Specifies the language to run the Monitor Agent in, using a two-letter language code as listed below. You must install the Monitor Agent in the selected language in order for the Monitor Agent to display in the selected language.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--lang *code*	/lang-*code*
Example:	--lang de	/lang-fr

The table below lists the valid language codes. Contact your local Novell sales office for information about language availability.

Language	Language Code	Language	Language Code
Arabic	AR	Hungarian	MA
Czechoslovakian	CS	Italian	IT
Chinese-Simplified	CS	Japanese	NI
Chinese-Traditional	CT	Korean	KR
Danish	DK	Norwegian	NO
Dutch	NL	Polish	PL

Language	Language Code	Language	Language Code
English-United States	US	Portuguese-Brazil	BR
Finnish	SU	Russian	RU
French-France	FR	Spanish	ES
German-Germany	DE	Swedish	SV
Hebrew	HE	Turkish	TR

/log

Specifies the full path of the directory where the Monitor Agent writes its log files. On Linux, the default directory is /var/log/novell/groupwise/gwmon. On Windows, the default is the GroupWise Monitor installation directory (typically c:\gwmon). See "Configuring Monitor Agent Log Settings" on page 925.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--log /*dir*/*file*	/log-[*drive*:]\dir\file /log-\\svr\sharename\dir\file
Example:	--log /opt/novell/groupwise/agents/logs	/log-\gw\logs /log-m:\gw\logs /log-\\\\server2\c\gw\logs

/pollthreads

Specifies the number of threads that the Monitor Agent uses for polling the agents for status information. Valid values range from 1 to 32. The default is 20. See "Configuring Polling of Monitored Agents" on page 917.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--pollthreads *number*	/pollthreads-*number*
Example:	--pollthreads 10	/pollthreads-32

/proxy

Routes all communication through the Monitor Agent and the Monitor Application (on the Web server). As long as the Web server can be accessed through the firewall, the Monitor Web console can receive information about all GroupWise agents that the Monitor Agent knows about. Without /proxy, the Monitor Web console cannot communicate with the GroupWise agents through a firewall. See "Configuring Proxy Service Support for the Monitor Web Console" on page 925.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--help	/help

XIV Client

73 Setting Up GroupWise Modes and Accounts

This section will familiarize you with GroupWise® modes and accounts, and help you set up users to use them.

- "GroupWise Modes" on page 965
- "Accounts" on page 972

GroupWise Modes

GroupWise provides three different ways to run the GroupWise client: Online mode, Caching mode, and Remote mode.

- "Online Mode" on page 965
- "Caching Mode" on page 965
- "Remote Mode" on page 967

NOTE: Remote mode is not available in the GroupWise Cross-Platform client.

Most GroupWise features are available in all three GroupWise modes, with a few exceptions. Subscribing to other users' notifications is not available in Caching mode. Subscribing to other users' notifications and Proxy are not available in Remote mode.

Online Mode

When users use Online mode, they are connected to their post office on the network. The user's mailbox displays the messages and information stored in the network mailbox (also called the Online Mailbox). Online mode is connected to the network mailbox continuously. In Online mode, if the Post Office Agent shuts down or users lose their network connection, they will (temporarily) lose the connection to their mailboxes.

Users should use this mode if they do not have a lot of network traffic, or if they use several different workstations and do not want to download a local mailbox to each one.

Caching Mode

Caching mode stores a copy of a user's network mailbox, including messages and other information, on the user's local drive. This allows GroupWise to be used whether or not the network or Post Office Agent is available. Because the user is not connected to the network all the time, this mode cuts down on network traffic and has the best performance. A connection is made automatically to retrieve and send new messages. All updates are performed in the background so GroupWise work is not interrupted.

Users should use this mode if they have enough disk space on the local drive to store their mailboxes.

Several users can set up their Caching Mailboxes on a single shared computer.

If users run Caching Mode and Remote Mode on the same computer, the same local mailbox (also called the Caching Mailbox or Remote Mailbox) can be used to minimize disk space usage.

If disk space is limited, users can restrict the items that are downloaded to the local mailbox. They can specify to get the subject line only or specify a size limit.

If users back up their Caching Mailbox, they can protect items that might be deleted if the system is set up to automatically clean up items (or if the system administrator runs an Expire and Reduce).

To use Caching mode, the client installation must be a standard installation, not a workstation installation.

Allowing or Forcing Use of Caching Mode

The system administrator can allow or disallow the use of Caching mode, and can also force users to log in to GroupWise in Caching mode.

If the system administrator forces Caching mode on Cross-Platform client users and then restricts Online mailbox size so that users have items in their Caching mailboxes that are no longer available online, the administrator needs to make sure users understand about doing backups. See "Backing Up Your Mailbox" in "Managing Your Mailbox" in the *GroupWise 6.5 Cross-Platform Client User Guide*.

1. In ConsoleOne®, click Tools > GroupWise Utilities > Client Options.
2. Click Environment > Client Access.
3. Select or deselect Allow Use of Caching Mode.
4. Select or deselect Force Use of Caching Mode.

   Specify the number of days before Caching mode will be enforced. This allows the user to continue using Online mode until the grace period has passed. The grace period begins the first time the user connects to the POA. The setting applies per user per workstation.

   The Force Caching Mode setting is not enforced on a workstation that does not have enough disk space for a Caching mailbox. The following amount of disk space is required: the size of the mailbox + 20 MB + 25% of the mailbox size.

   The Force Caching Mode setting is also not enforced when a user connects from a shared Windows workstation or terminal server if you configure these workstations to be excluded. You do this by setting a registry key on the Windows workstation. The registry key is in HKEY_LOCAL_MACHINE. Under Software\\Novell\\GroupWise\\Client, add a dword value named No Local Store with a value of 1. This will prevent the user from creating a Caching or Remote mailbox by using the GroupWise Windows client menus. However, the user can still create a Caching or Remote mailbox by using the startup switches /pc, /pr, or /ps.

Downloading the System Address Book

When users prime their Caching mailboxes, they receive a copy of the system address book. After the initial priming of the Caching mailbox, users can re-download the system address book and their personal address books in Caching mode by clicking View > Retrieve System Address Book or View > Retrieve Personal Address Book while in the Address Book. Address books will also be re-downloaded in Caching mode when users click Tools > Retrieve Entire Mailbox.

Users can also specify to download the system address book (and any rules they have created) on a regular basis. In Remote or Caching mode, click Accounts > Account Options. Right-click the GroupWise account, then click Properties > Advanced. Select Refresh Address Books and Rules Every __ Days. By default this is set to 7 days, but can be changed.

If you configure the POA to generate the system address book regularly, Caching mode users will always have a current copy to download. In ConsoleOne, right-click the POA object, then click Properties > GroupWise > Maintenance. On the Maintenance page, make sure that Generate Address Book for Remote is selected. You can choose the time when you want the generation to take place.

If you want to generate the system address book for download more often than once a day, you can delete the existing wprof50.db file from the \wpcsout\ofs subdirectory of each post office. A new downloadable system address book will be generated automatically for users on each post office.

Remote Mode

Remote mode is familiar to GroupWise users on the road. Similar to Caching mode, a copy of the Online mailbox, or the portion of the mailbox that users specify, is stored on the local drive. Users can periodically retrieve and send messages with the type of connection they specify (modem, network, or TCP/IP). Users can restrict what is retrieved, such as only new messages or only message subject lines.

NOTE: Remote mode is not available in the GroupWise Cross-Platform client.

To use Remote mode, the Windows client installation must be a standard (full) installation, not a workstation installation.

As an administrator, you can allow or disallow the use of Remote mode for client users.

1. In ConsoleOne, click Tools > GroupWise Utilities > Client Options.
2. Click Environment > Client Access.
3. Select or deselect Allow Use of Remote Mode.

The following topics explain the capabilities users have when they are allowed to use Remote mote.

- "Remote Password" on page 967
- "Async Gateway and X.25 Gateway" on page 968
- "Remote Performance" on page 968
- "Hit the Road" on page 968
- "Remote Properties" on page 968
- "Remote Mode Connections" on page 969

Remote Password

To use Remote mode, users must have a password set in Online mode. When they run in Remote mode for the first time, they can specify to use the same password in Remote mode or choose a new one.

Async Gateway and X.25 Gateway

For GroupWise to use a modem connection, the GroupWise Async Gateway or X.25 Gateway must be installed and configured in your GroupWise system. The gateway provides the means by which the client communicates with the GroupWise system.

Remote Performance

The system administrator can configure the MTA so that it re-directs Remote mode requests to other MTAs and POAs. The GroupWise client can establish a client/server connection to an MTA across the Internet. For more information, see "Enabling Live Remote" on page 589.

Hit the Road

Users can use Hit the Road on the Tools menu (or switch from Online mode to Remote mode) to create, set up, or update the Remote mailbox. A copy of the mailbox is created on the user's local drive and any current connections are detected and set up. If users have already used Caching mode, the local mailbox has already been created. Users can also use Hit the Road to create setup files on a diskette to set up their Remote mailbox on a computer that's not connected to the network. Several users can set up their Remote mailboxes on a single shared computer.

Hit the Road creates a network connection for the method (direct connection or TCP/IP) GroupWise uses to access the user's post office. GroupWise can then use this connection, when running in Remote mode, to connect to the GroupWise system. For example, a network connection lets users of docked laptops run GroupWise in Remote mode and connect to the GroupWise system through the network connection rather than a modem connection.

Hit the Road also creates modem connections for Remote Profiles in the Async Gateway or X.25 Gateway. Remote Profiles let GroupWise connect to the GroupWise system.

To use Hit the Road:

1. In the GroupWise client, click Tools > Hit the Road.
2. Follow the prompts to create the Remote mailbox on the computer or on a diskette.

Installing the Remote Mailbox from Diskette

If Hit the Road created the user's Remote mailbox on diskette, the user needs to install the Remote mailbox on the computer that will be running in Remote mode.

1. Insert the diskette containing the Remote mailbox into the computer's disk drive.
2. From the Windows Taskbar, click Start > Run.
3. Type `a:\setup`, then click OK.

   Follow the prompts. The setup program creates a Remote mailbox and copies the required files to the computer's hard drive.

Remote Properties

Users can change the way Remote mode is set up, including the connection, time zone, signature, and so forth, in Account Options on the Accounts menu. Remote is listed as an account.

By default, if an item is deleted from the Remote mailbox, the item will be deleted from the Online mailbox the next time a connection is made. Deletion options in Remote Properties can be changed so that an item deleted from the Remote mailbox will stay in the Online mailbox or vice versa.

Remote Mode Connections

- "Setting Up a Modem Connection" on page 969
- "Setting Up a Network Connection" on page 970
- "Setting Up a TCP/IP Connection" on page 971

Setting Up a Modem Connection

If you are going to connect with a modem, you must create at least one modem connection. A modem connection provides GroupWise with the information it needs to connect to the GroupWise system through the GroupWise Async Gateway or GroupWise X.25 Gateway.

To set up a modem connection:

1. In the client, log in or change to Remote mode.
2. Click Accounts > Send/Retrieve > GroupWise Options.
3. Click Configure > Connect To > New.
4. Make sure Modem is selected, then click OK.
5. Type a descriptive name for the modem connection in the Connection Name box.
6. Click the country code, then type the area code and phone number for the gateway to the master GroupWise system.

   You can use a comma (,) to signal a one-second pause in dialing such as 9, (800) 555-5555. The 9 accesses an outside line and the comma causes a one-second pause to wait for the dial tone before dialing the number. If you enter dashes, spaces, and parentheses, they are ignored.
7. Type the login ID for the gateway.
8. Click Password, type the gateway password, then click OK.
9. Retype the password, then click OK.
10. Click the Advanced tab.
11. If your modem requires a script, specify the path to the script in the Modem Script box, click Edit Script, then specify the necessary When Given and Respond With commands.

    To save the script without changing its filename, click Save > Close.

    or

    To save the script with a new filename, click Save As, type a name, then click Close.
12. Click a disconnect method.

Method	Description
When All Updates Are Received	Disconnects after requests are sent and after all responses to the requests are received (or disconnects automatically when the time allowed by the gateway has expired).
Do Not Wait for Responses	Disconnects immediately after requests are sent and pending responses are received. Pending responses are responses to other requests that are waiting to be downloaded to you.
Manually	Lets you manually control when to disconnect (or disconnects automatically when the time allowed by the gateway has expired).

13 Click Attempts, then specify the number of times to redial if the line is busy.

14 Click Retry Interval, then specify the time interval between each redial attempt.

15 Click OK.

16 Select the connection you want, then click Select.

17 Select the location you are connecting from in the Connecting From box. If none are listed, use the Default Location option.

If you need to create a new location, click the Connect From button. This is useful for laptop users who are calling into the GroupWise system from different geographic locations.

18 Select the modem to use for dialing up the gateway in the Connect Using box. If you have not yet defined your modem, click Modem to add a modem to your system.

19 Click OK, then click Close.

Setting Up a Network Connection

While running in Remote mode, GroupWise can connect to the user's Online mailbox using a network connection. A network connection is useful for laptop users connecting to the network through a docking station, or for remote users connecting through a modem using remote node software.

To create a network connection:

1 In the client, log in or change to Remote mode.

2 Click Accounts > Send/Retrieve > GroupWise Options.

3 Click Network > OK.

4 Type a descriptive name for the network connection in the Connection Name box.

5 Type the path to any post office directory in the master GroupWise system.

Users can connect to their own post offices or to any post office in the master GroupWise system to access their Online mailboxes.

6 Click a disconnect method.

Method	Description
When All Updates Are Received	Disconnects after requests are sent and after all responses to the requests are received (or disconnects automatically when the time allowed by the gateway has expired).
Do Not Wait for Responses	Disconnects immediately after requests are sent and pending responses are received. Pending responses are responses to other requests that are waiting to be downloaded to you.
Manually	Lets you manually control when to disconnect (or disconnects automatically when the time allowed by the gateway has expired).

7 Click OK.

8 Select the connection you want, then click Select.

9 Select the location you are connecting from in the Connecting From box. If none are listed, use the Default Location option.

If you need to create a new location, click the Connect From button. This is useful for laptop users who are calling into the GroupWise system from different geographic locations.

10 Click OK > Close.

Setting Up a TCP/IP Connection

A TCP/IP connection enables GroupWise, while running in Remote mode, to connect to the GroupWise system through a network connection using TCP/IP rather than a modem connection. A TCP/IP connection can be made through a network connection, such as a laptop connecting to the network through its docking station, or through a modem using remote node software.

To create a TCP/IP connection:

1 In the client, log in or change to Remote mode.

2 Click Accounts > Account Options, then double-click the Remote account.

3 Click Connection > Connect To > New > TCP/IP > OK.

4 Type a descriptive name for the TCP/IP connection.

5 Type the IP address or the DNS name.

6 Type the IP port for this address.

7 Click a disconnect method.

Method	Description
When All Updates Are Received	Disconnects after requests are sent and after all responses to the requests are received (or disconnects automatically when the time allowed by the gateway has expired).
Do Not Wait for Responses	Disconnects immediately after requests are sent and pending responses are received. Pending responses are responses to other requests that are waiting to be downloaded to you.
Manually	Lets you manually control when to disconnect (or disconnects automatically when the time allowed by the gateway has expired).

8 Click OK.

9 Select the connection you want, then click Select.

10 Select the location you are connecting from in the Connecting From box. If none are listed, use the Default Location option.

If you need to create a new location, click the Connect From button. This is useful for laptop users who are calling into the GroupWise system from different geographic locations.

11 Click OK > Close.

Accounts

- "Accounts Menu" on page 972
- "Enabling POP3, IMAP4, and NNTP Account Access in Online Mode" on page 972

Accounts Menu

In addition to the Remote account, users can access and configure POP3 and IMAP4 Internet e-mail accounts and NNTP News accounts from the Accounts menu. While the user is in Remote and Caching mode, POP3, IMAP4, and NNTP accounts are accessed without needing to connect to the GroupWise system. If the system administrator enables it, users can also access and configure their POP3, IMAP4, and NNTP accounts from the Accounts menu while in Online mode.

NOTE: The Accounts menu is not available in the GroupWise Cross-Platform client.

Enabling POP3, IMAP4, and NNTP Account Access in Online Mode

By default, POP3, IMAP4, and NNTP accounts can be added, configured, and accessed by users in Remote and Caching mode only. Account items and information are not accessible in Online mode, nor can items and information be uploaded to the Online mailbox until the system administrator enables it.

To enable POP3, IMAP4, and NNTP account access in client users' Online mode for an entire post office:

1. Make sure GroupWise 6.*x* agents have been installed. For more information, see "Message Transfer Agent" on page 555.
2. Make sure Internet Addressing is enabled. For more information, see "Internet Addressing" on page 61.
3. In ConsoleOne, select the post office object.
4. Click Tools > GroupWise Utilities > Client Options.
5. Click Environment > General.
6. Select Allow Use of POP and IMAP Accounts in the Online Mailbox.
7. Select Allow Use of News (NNTP) Accounts in the Online Mailbox.
8. Click OK.

74 Setting Defaults for the GroupWise Client Options

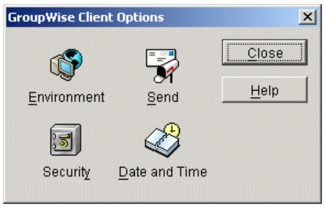
The GroupWise® client includes options (preferences) that can be set by individual users. As a GroupWise administrator, you can determine the default settings for the options. If you don't want users to change the default settings you've established, you can lock the settings.

- "Client Options Summary" on page 973
- "Setting Client Options" on page 976
- "Resetting Client Options to Default Settings" on page 1002

Client Options Summary

Default settings can be established at the user level, the post office level, or the domain level. User settings override post office settings, and post office settings override domain settings.

1 In ConsoleOne®, select a Domain, Post Office, or User object, then click Tools > GroupWise Utilities > Client Options.



The client options table in this section summarizes all client options and provides links to descriptions of the options. For more detailed instructions, see "Setting Client Options" on page 976.

- Environment
- Send
- Security
- Date and Time

NOTE: The Cross-Platform client does not recognize all of the client options that can be set in ConsoleOne. Client options that the Cross-Platform client does recognize are marked with an asterisk (*) in the table.

Client Options Type	Client Options Tab	Client Options
Environment Click Tools > GroupWise Utilities > Client Options > Environment	General	Refresh Interval Allow Shared Folder Creation Allow Shared Address Book Creation Check Spelling Before Send Junk Mail Handling Enable Junk Mail Handling Enable Junk Mail Using Junk Mail Lists Enable Junk Mail Using Personal Address Books Auto-Delete After __ Days Enable Blocked Mail Using Block Mail Lists Allow Use of POP and IMAP Accounts in the Online Mailbox Allow Use of News (NNTP) Accounts in the Online Mailbox
	Client Access	Client Licensing Full License Mailboxes Limited License Mailboxes Client Login Mode Allow Use of Remote Mode Allow Use of Caching Mode Force Caching Mode after __ Days Show Login Mode Drop-Down List on Client Toolbar
	Views	View Options Read Next After Accept, Decline, or Delete Open New View after Send Disable HTML View
	File Location	Archive Directory Custom Views
	Cleanup	Mail and Phone Manual Delete and Archive Auto-Delete After Auto-Archive After Appointment, Task, and Note Manual Delete and Archive Auto-Delete After Auto-Archive After Empty Trash Manual Automatic After Allow Purge of Items Not Backed Up Prompt before Purging
	Threshold	Operations
	Retention	Retention

Client Options Type	Client Options Tab	Client Options
Send Click Tools > GroupWise Utilities > Client Options > Send	Send Options	Classification* Normal, Proprietary, Confidential, Secret, Top Secret, For Your Eyes Only Priority* High, Standard, Low Reply Requested* When Convenient, Within __ Days Allow Use of Reply to All in Rules Allow Use of Internet Mail Tracking Expiration Date Delay Delivery Wildcard Addressing Notify Recipients Convert Attachments Allow Reply Rules to Loop
	Mail	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification* When Opened/Deleted None, Mail Receipt, Notify, Notify and Mail
	Appointment	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification* When Opened/Accepted/Deleted None, Mail Receipt, Notify, Notify and Mail
	Task	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification* When Opened/Accepted/Completed/Deleted None, Mail Receipt, Notify, Notify and Mail
	Note	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification* When Opened/Deleted None, Mail Receipt, Notify, Notify and Mail
	Security	Conceal Subject Require Password to Complete Routed Item Secure Items Options Do Not Allow Use of S/MIME* URL for Certificate Download Sign Digitally* Encrypt for Recipients Encryption Key Size
	Disk Space Management	User Limits Mailbox Size Limit Threshold for Warning Users Maximum Send Message Size

Client Options Type	Client Options Tab	Client Options
Security Click Tools > GroupWise Utilities > Client Options > Security	Password	Enter New Password* Clear User Password* Allow Password Caching Allow eDirectory Authentication Instead of Password Enable eDirectory Single Sign-On
	Macros	View Macro Security Always Play Received Macros Never Play Received Macros Always Prompt Before Playing a Macro
	Notify	Check for Mail Every
Date and Time Click Tools > GroupWise Utilities > Client Options > Date and Time	Calendar	Month Display Option First of Week Highlight Day Show Week Number Appointment Options Include Myself on New Appointments Display Appointment Length As Duration, End Date and Time Default Length Alarm Options Set Alarm When Accepted Default Alarm Time Work Schedule Start/End Time Work Days
	Busy Search	Appointment Length Range and Time to Search Days to Search

Setting Client Options

Default settings can be established at the user level, the post office level, or the domain level. User settings override post office settings, and post office settings override domain settings. However, if you set a lock on an option at a higher level, the higher level then overrides the setting for the lower level.

To modify the default settings for the GroupWise client:

1. In ConsoleOne, click a Domain object if you want to modify the settings for all users in the domain.

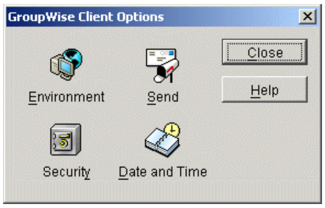
   or

   Click a Post Office object if you want to modify the settings for all users in the post office.

   or

   Click a User object or GroupWise External Entity object if you want to modify settings for the individual user. To change the same settings for multiple users, select multiple objects.

2. With the appropriate GroupWise object selected, click the Tools menu > click GroupWise Utilities > click Client Options to display the GroupWise Client Options dialog box.



3 To set the Environment options, click Environment > continue with "Modifying Environment Options" on page 977.

or

To set the Send options, click Send > skip to "Modifying Send Options" on page 987.

or

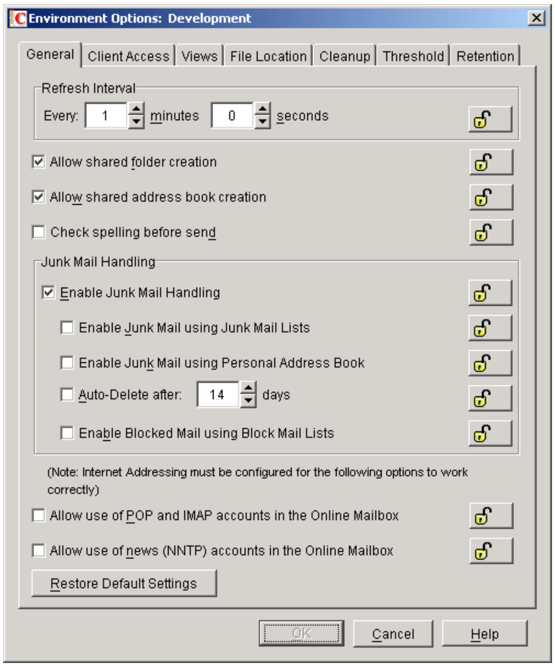
To set the Security options, click Security > skip to "Modifying Security Options" on page 996.

or

To set the Date and Time options, click Date and Time > skip to "Modifying Date and Time Options" on page 999.

Modifying Environment Options

1 If the Environment Options dialog box is not displayed, follow the instructions in "Setting Defaults for the GroupWise Client Options" on page 973 to display the dialog box.



Refresh Interval

Every: 1 minutes 0 seconds

☑ Allow shared folder creation

☑ Allow shared address book creation

☐ Check spelling before send

Junk Mail Handling

☑ Enable Junk Mail Handling

☐ Enable Junk Mail using Junk Mail Lists

☐ Enable Junk Mail using Personal Address Book

☐ Auto-Delete after: 14 days

☐ Enable Blocked Mail using Block Mail Lists

(Note: Internet Addressing must be configured for the following options to work correctly)

☐ Allow use of POP and IMAP accounts in the Online Mailbox

☐ Allow use of news (NNTP) accounts in the Online Mailbox

2 Click the tab that contains the options you want to change. Refer to the following sections for information about options:

"Environment Options: General" on page 978
"Environment Options: Client Access" on page 980
"Environment Options: Views" on page 982

“Environment Options: File Locations” on page 982

“Environment Options: Cleanup” on page 983

“Environment Options: Threshold” on page 985

NOTE: The Environment options are not currently recognized by the Cross-Platform client.

3. If you want to prevent users from changing an option’s setting, click the lock button next to it.

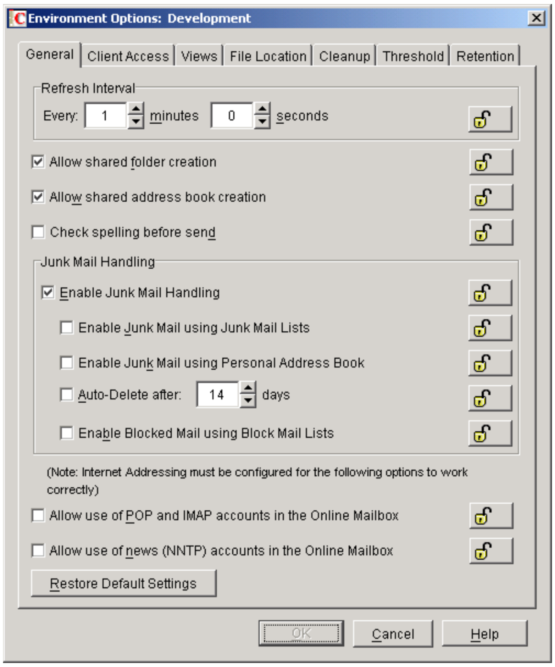
   After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.

4. If you want to return all the options on a tab to their default settings, click Restore Default Settings.

5. When finished, click OK to save your changes.

Environment Options: General

The General options determine such settings as the refresh interval for new messages, whether users can create shared folders and address books, and which types of accounts can be used while in Online mode.



Environment Options: Development

Refresh Interval

Every: 1 minutes 0 seconds

☑ Allow shared folder creation

☑ Allow shared address book creation

☐ Check spelling before send

Junk Mail Handling

☑ Enable Junk Mail Handling

☐ Enable Junk Mail using Junk Mail Lists

☐ Enable Junk Mail using Personal Address Book

☐ Auto-Delete after: 14 days

☐ Enable Blocked Mail using Block Mail Lists

(Note: Internet Addressing must be configured for the following options to work correctly)

☐ Allow use of POP and IMAP accounts in the Online Mailbox

☐ Allow use of news (NNTP) accounts in the Online Mailbox

Refresh Interval

This option determine how often the GroupWise client lists will be updated to reflect new message status. The default is 1 minute.

Allow Shared Folder Creation

Select this option to enable users to share folders with other users. By default, this option is enabled.

Allow Shared Address Book Creation

Select this option to enable users to share address books with other users. By default, this option is enabled.

Check Spelling Before Send

Select this option to have the message text of each item automatically spell checked before the item is sent. By default, this option is disabled.

Junk Mail Handling

Choose from the following settings to determine what Junk Mail Handling options are available to client users.

- **Enable Junk Mail Handling:** Select this option to make the Junk Mail Handling feature available for a user. This setting affects both the client and the POA. Junk Mail Handling allows users to block or "junk" unwanted Internet e-mail. When this setting is enabled, the client will display Junk Mail Handling menus and dialog boxes, and the POA will perform Junk Mail Handling if the block and junk lists are also enabled.

  When this setting is disabled, the client will not display any Junk Mail Handling menus or dialog boxes, and the POA will not perform any Junk Mail Handling for the user.

- **Enable Junk Mail Using Junk Mail Lists:** Select this option to make junking available to users. A user can junk e-mail from an Internet e-mail address or Internet domain, when the e-mail addresses and Internet domains are listed in the user's Junk List. (Initially, there are no entries in a user's junk list.) Junked items are delivered to the Junk Mail folder in the user's Mailbox.

  When this setting is enabled or disabled and not locked, the user's initial setting to use the Junk List will be enabled or disabled. Users can change the setting. When enabled and locked, a user's Enable Junk List setting is enabled and cannot be disabled. When disabled and locked, the Junk List will be unavailable to the user. Client menu options and dialogs involving the Junk List will not be displayed.

- **Enable Junk Mail Using Personal Address Book:** Select this option to allow users' personal address books to function like Junk Lists. All items from e-mail addresses not in users' Frequent Contacts address book and other personal address books will be delivered to the Junk Mail folder in the user's Mailbox.

  When this setting is enabled or disabled and not locked, the user's initial setting to use personal address books will be enabled or disabled. Users can change the setting. When enabled and locked, a user's Enable Junk Mail Using Personal Address Books setting is enabled and cannot be disabled. When disabled and locked, the personal address books option will be unavailable to the user. Client menu options and dialog boxes involving personal address books will not be displayed.

- **Auto-Delete After __ Days:** Select this option to automatically delete items from the Junk Mail folder. Specify the number of days after which items should be deleted.

- **Enable Blocked Mail Using Block Mail Lists:** Select this option to make blocking available to users. A user can block e-mail from an Internet e-mail address or Internet domain, when blocked e-mail addresses and Internet domains are listed in the user's Block List. (Initially, there are no entries in a user's Block List.) Blocked items are blocked when the POA processes delivery to the user's mailbox, and the items are never delivered to the user's mailbox. When the POA log uses Verbose mode, the log will display information about blocked items.

When this setting is enabled or disabled and not locked, the user's initial setting to use the Block List will be enabled or disabled. Users can change the setting. When enabled and locked, a user's Block List setting is enabled and cannot be disabled. When disabled and locked, blocking will be unavailable to the user. Client menu options and dialog boxes involving the Block List will not be displayed.

Allow Use of POP and IMAP Accounts in the Online Mailbox

Select this option to enable users to access POP and IMAP accounts while using the GroupWise client in Online mode.

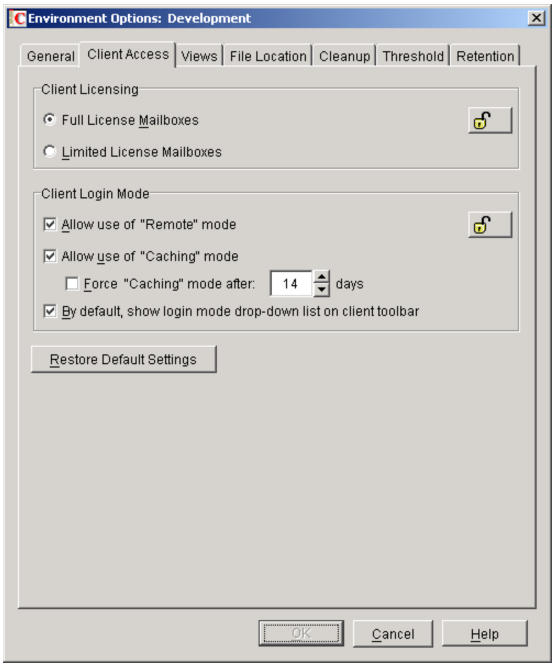
By default, this option is disabled. If you enable this option, an Accounts menu is added to the GroupWise client, allowing users to add POP and IMAP accounts to GroupWise, set account properties, and send and retrieve items from their POP and IMAP accounts. In addition, users are allowed to upload POP and IMAP items from the Remote mailbox to the Online mailbox.

Allow Use of News (NNTP) Accounts in the Online Mailbox:

Select this option to enable users to set up newsgroup (NNTP) accounts while using the GroupWise client in Online mode.

Environment Options: Client Access

The Client Access options allow you to apply a license type (full or limited) to users' mailboxes and enable/disable the Remote and Caching modes in the GroupWise client for Windows.



Environment Options: Development

Client Licensing

● Full License Mailboxes

○ Limited License Mailboxes

Client Login Mode

☑ Allow use of "Remote" mode

☑ Allow use of "Caching" mode

□ Force "Caching" mode after: 14 days

☑ By default, show login mode drop-down list on client toolbar

Client Licensing

GroupWise offers two types of mailbox licenses: full client mailbox licenses and limited client mailbox licenses.

A full client mailbox license has no mailbox access restrictions; the mailbox can be accessed by any GroupWise client (Windows or WebAccess) as well as any third-party plug-in or POP/IMAP client.

A limited client mailbox license restricts mailbox access to the following:

- The GroupWise WebAccess client (including wireless devices)
- A GroupWise client (Windows or WebAccess) via the Proxy feature
- A GroupWise client (Windows or WebAccess) via the Busy Search feature
- A POP or IMAP client

Note that a limited client license mailbox does not allow access through the GroupWise client for Windows (other than via Proxy or Busy Search).

You can use this option to specify the type of client license that you want applied to users' mailboxes. This enables you to support the type of GroupWise mailbox licenses you've purchased. For example, if you've only purchased limited client license mailboxes for users on a specific post office, you can mark all mailboxes on that post office as being limited client license mailboxes.

For information about generating an audit report that shows the type of license applied to each mailbox in a post office, see "Auditing Mailbox License Usage in the Post Office" on page 180.

Client Login Mode

Choose from the following settings to determine which login modes are available to GroupWise users when using the GroupWise client for Windows. These settings apply only if you selected Full License Mailboxes for the client licensing.

- **Allow Use of Remote Mode:** Select this option to enable users to log in with GroupWise in Remote mode. With Remote mode, the GroupWise client uses a Remote mailbox on the user's local drive. The user must initiate a connection (modem, direct, or TCP/IP) to send or retrieve items from the GroupWise system. For more information about Remote mode, see "Remote Mode" on page 967. By default, this option is enabled.

  NOTE: Remote Mode is not available in the Cross-Platform client.

- **Allow Use of Caching Mode:** Select this option to enable users to log in with GroupWise in Caching mode. With Caching mode, the GroupWise client uses a Caching mailbox on the user's local drive (this can be the same mailbox as the Remote mailbox). The GroupWise client periodically initiates a connection with the GroupWise system to send and receive items. For more information about Caching mode, see "Caching Mode" on page 965. By default, this option is enabled.

  Select the Force Caching Mode option (available only if the Allow Use of Caching Mode option is enabled) to force users to run in Caching mode. By default, this option is disabled. Specify the number of days before Caching mode will be enforced. This allows the user to continue using Online mode until the grace period has passed. The grace period begins the first time the user connects to the POA. The setting applies per user per workstation.

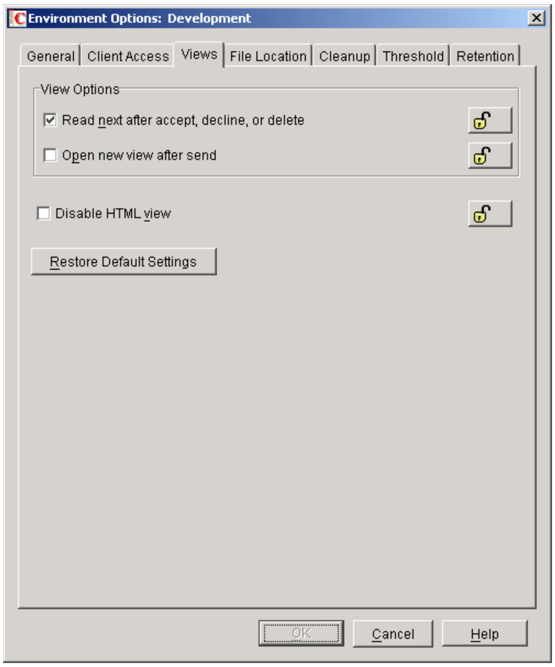
  The Force Caching Mode setting is not enforced on a workstation that does not have enough disk space for a Caching mailbox. The following amount of disk space is required: the size of the mailbox + 20 MB + 25% of the mailbox size.

  The Force Caching Mode setting is also not enforced when a user connects from a shared Windows workstation or terminal server if you configure these workstations to be excluded. You do this by setting a registry key on the Windows workstation. The registry key is in HKEY_LOCAL_MACHINE. Under Software\\Novell\\GroupWise\\Client, add a dword value named No Local Store with a value of 1. This will prevent the user from creating a Caching or Remote mailbox by using the GroupWise Windows client menus. However, the user can still create a Caching or Remote mailbox by using the startup switches /pc, /pr, or /ps.

- **By Default, Show Login Mode Drop-Down List on Client Toolbar:** Select this option to have the Login Mode drop-down list displayed on the client's toolbar. This enables users to change the mode themselves and is only necessary if you allow multiple modes to be used. By default, this option is enabled.

Environment Options: Views

The Views Environment options determine when items open, and whether or not users can read and compose messages in HTML.



View Options

☑ Read next after accept, decline, or delete

□ Open new view after send

□ Disable HTML view

View Options

Choose from the following settings to determine what occurs when the user performs an action that closes the current view.

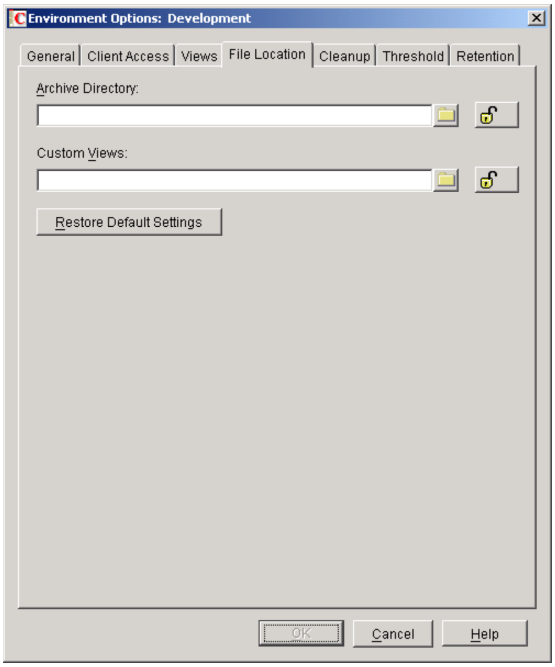
- **Read Next after Accept, Decline, or Delete:** Select this option to have the next available received item automatically open after the user accepts, declines, or deletes an appointment, task, or note. By default, this option is enabled.
- **Open New View after Send:** Select this option to have a new send view open after a user sends a message. By default, this option is disabled.

Disable HTML View

Turns off the ability to view or compose messages in HTML View.

Environment Options: File Locations

The File Locations options determine the locations of users' archive directories and the custom views directory.



Archive Directory

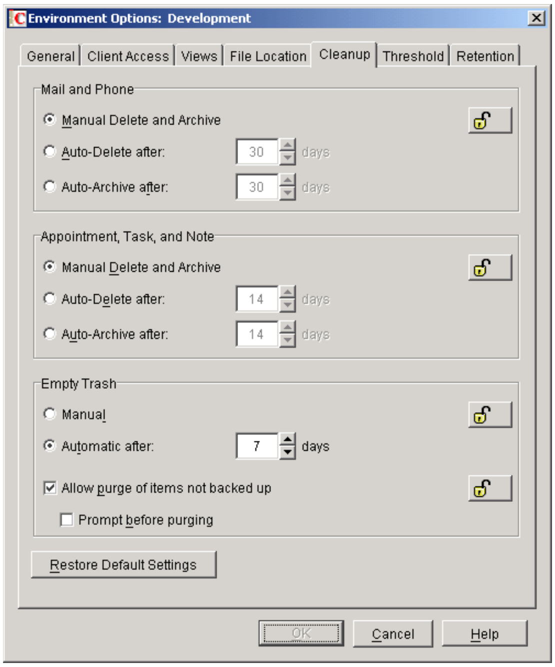
Select the directory to be used for archiving items. Each user must have his or her own archive directory, so this can be a local directory (for example, c:\novell\groupwise) or a personal user directory on a network server. If you select a local drive, make sure users have the directories created. If you select a network drive, make sure users have the necessary rights to access the directories.

Custom Views

This option applies only if you are using custom views. Select the directory where the views are located. The GroupWise product does not include the capability to design custom views, but third-party products make use of this feature to support their specialized capabilities.

Environment Options: Cleanup

The Cleanup options determine the delete and archive settings for GroupWise items (mail messages, phone messages, appointments, tasks, and notes).



Mail and Phone

● Manual Delete and Archive

○ Auto-Delete after: 30 days

○ Auto-Archive after: 30 days

Appointment, Task, and Note

● Manual Delete and Archive

○ Auto-Delete after: 14 days

○ Auto-Archive after: 14 days

Empty Trash

○ Manual

● Automatic after: 7 days

☑ Allow purge of items not backed up

□ Prompt before purging

Mail and Phone

Choose from the following settings to determine how mail and phone messages are deleted and archived:

- **Manual Delete and Archive:** Select this option to have mail and phone messages deleted or archived only when users manually do it. This is the default setting.
- **Auto-Delete After:** Select this option to have GroupWise automatically delete mail and phone messages that are older than the specified number of days. If you use this option, you should notify users so they know they must archive items they want to save.
- **Auto-Archive After:** Select this option to have GroupWise archive mail and phone messages that are older than the specified number of days. Users must have an archive directory specified in order for items to be archived. See "Environment Options: File Locations" on page 982 for information about setting a default archive directory location.

Appointment, Task, and Note

Choose from the following settings to determine how appointments, tasks, and notes are deleted or archived:

- **Manual Delete and Archive:** Select this option to have appointments, tasks, and notes deleted or archived only when users manually do it. This is the default setting.
- **Auto-Delete After:** Select this option to have GroupWise automatically delete appointments, tasks, or notes that are older than the specified number of days. If you use this option, you should notify users so they know they must archive items they want to save.
- **Auto-Archive After:** Select this option to have GroupWise automatically archive appointments, tasks, and notes older than the specified number of days. Users must have an archive directory specified in order for items to be archived. See "Environment Options: File Locations" on page 982 for information about setting a default archive directory location.

Empty Trash

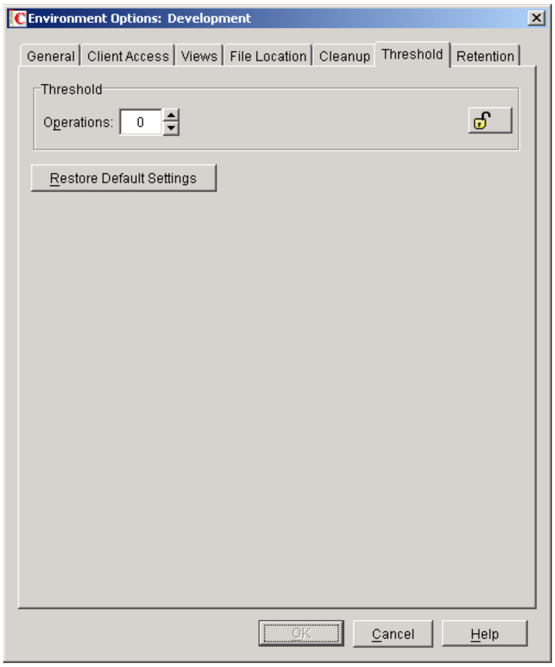
Deleted items are moved to the Trash folder. They can be retrieved from the Trash until it is emptied. Items in the Trash still take up disk space. Select from the following settings to determine how the Trash folder is emptied:

- **Manual:** Select this option to require the user to manually empty the Trash. This is the default setting.
- **Automatic:** Select this option to have GroupWise automatically empty items from the trash after they have been in it for the specified number of days.
- **Allow Purge of Items Not Backed Up:** Select this option to enable items that have not been backed up to be removed from the trash. This option is enabled by default.

  Select the Prompt Before Purging option (available only if Allow Purge of Items Not Backed Up is enabled) to prompt the user to confirm the purging of any files that have not been backed up.

Environment Options: Threshold

The Threshold option lets you determine how much work the GroupWise client performs versus how much work it offloads to the Post Office Agent (POA).



Environment Options: Development

Threshold

Operations: 0

Operations

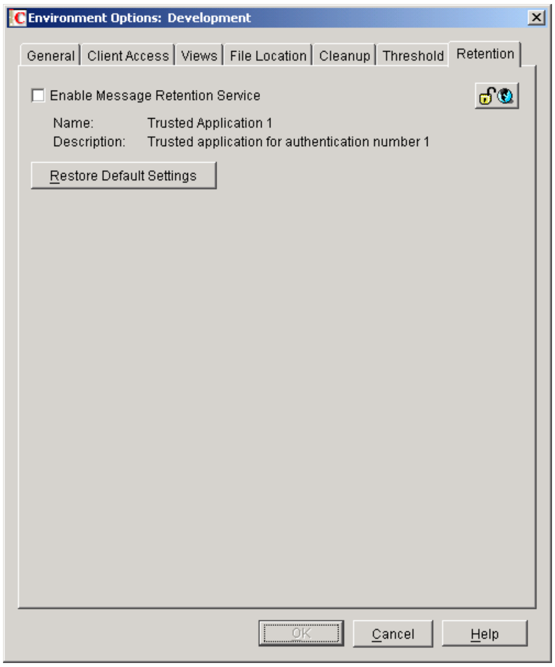
Set the number of operations for the GroupWise client to perform before offloading message delivery to the POA. The default is 0, which means that all message delivery will be offloaded to the POA.

The Threshold can be set only by the administrator and cannot be changed by users.

Environment Options: Retention

The Retention tab is displayed only if the Provides Message Retention Service setting is turned on for a trusted application. For information, see "Trusted Applications" on page 62.

Message retention is configurable by administrators only, not by GroupWise users. The Retention options do not display in the GroupWise client.



□ Enable Message Retention Service

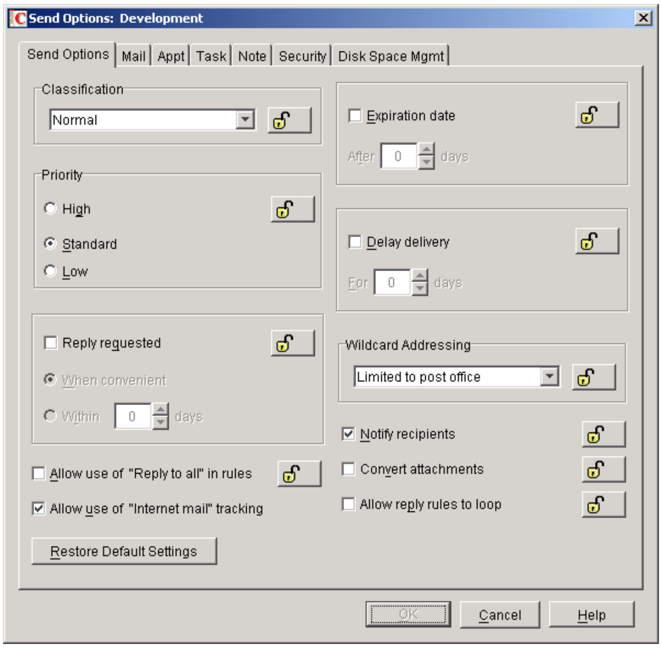
Name: Trusted Application 1
Description: Trusted application for authentication number 1

Enable Message Retention Service

Select this option to enable the Message Retention Service. If you are setting client options for a domain, all user mailboxes in the domain will support message retention. Likewise, if you are setting options for a post office, all users in the post office will support message retention. Once a user's mailbox is enabled for message retention, the user can not perform any action (purging, archiving, etc.) that removes messages from the mailbox until the messages have been copied to another storage location by a trusted application that has been designed to provide the Message Retention Service.

Modifying Send Options

1 If the Send Options dialog box is not displayed, follow the instructions in "Setting Defaults for the GroupWise Client Options" on page 973 to display the dialog box.



Classification: Normal

Priority: ○ High ● Standard ○ Low

□ Reply requested

● When convenient

○ Within 0 days

□ Allow use of "Reply to all" in rules

☑ Allow use of "Internet mail" tracking

□ Expiration date

After 0 days

□ Delay delivery

For 0 days

Wildcard Addressing: Limited to post office

☑ Notify recipients

□ Convert attachments

□ Allow reply rules to loop

2 Click the tab that contains the options you want to change. Refer to the following sections for information about options:

"Send Options: Send Options" on page 987

"Send Options: Mail" on page 990

"Send Options: Appointment" on page 991

"Send Options: Task" on page 992

"Send Options: Task" on page 992

"Send Options: Note" on page 993

"Send Options: Security" on page 994

"Send Options: Disk Space Management" on page 995

NOTE: To determine which Send options are recognized by the Cross-Platform client, refer to the client options table in "Client Options Summary" on page 973.

3 If you want to prevent users from changing an option's setting, click the lock button next to it.

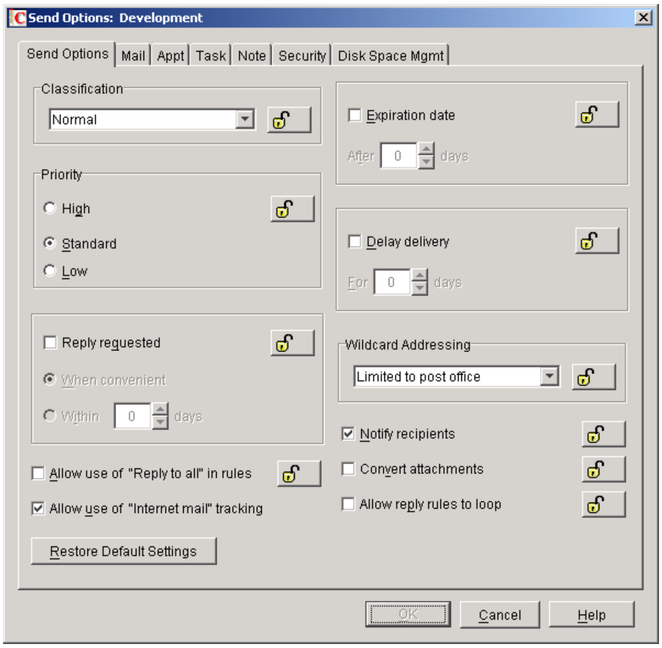
After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.

4 If you want to return all the options on a tab to their default settings, click Restore Default Settings.

5 When finished, click OK to save your changes.

Send Options: Send Options

The Send Options determine general settings that apply to all GroupWise item types (mail messages, phone messages, appointments, tasks, and notes).



Classification: Normal

Priority: ○ High ● Standard ○ Low

□ Reply requested

● When convenient

○ Within 0 days

□ Allow use of "Reply to all" in rules

☑ Allow use of "Internet mail" tracking

□ Expiration date

After 0 days

□ Delay delivery

For 0 days

Wildcard Addressing: Limited to post office

☑ Notify recipients

□ Convert attachments

□ Allow reply rules to loop

Classification

Select the default for the security classification label at the top of the message box. It does not provide any encryption or additional security. It is meant to alert the recipient to the relative sensitivity of the item. The options are Normal, Proprietary, Confidential, Secret, Top Secret, and For Your Eyes Only. The default is Normal.

Priority

Select High, Standard, or Low as the default item priority. Priority determines which post office directory an item is placed in. This, in turn, determines how quickly items will be delivered. High priority items will be queued ahead of normal or low priority items.

Reply Requested

Select the Reply Requested option to have items always include a reply request. By default, this option is disabled. If you enable the option, select whether the recipient will be asked to reply when it is convenient or within a specific number of days.

Allow Use of Reply to All in Rules

Select this option to enable users to use the Reply to All action when creating rules. By default, this option is disabled, which means that only the Reply to Sender action is available.

Allow Use of Internet Mail Tracking

Select this option to allow users' GroupWise clients to automatically embed information in Internet-bound items. The embedded information instructs the receiving system to send back a delivery notification message (if it is supported). By default, this option is enabled.

To make Internet Status Tracking work, users must also turn on the setting in the GroupWise client (Tools menu > Options > Send Options > Mail > Enable Delivery Confirmation). By default, the Enable Delivery Confirmation is turned off in the GroupWise client.

Expiration Date

Select this option to have unopened messages expire after the specified number of days. By default, this option is disabled.

Delay Delivery

Select this option to delay the delivery of messages for the specified number of days. For example, if you specify 3 days, a message will not be delivered until 3 days after the day it is sent. Messages will be delivered at 12:01 a.m. of the appropriate day. By default, this option is disabled.

Wildcard Addressing

Wildcard addressing enables a user to send an item to all users in a post office, domain, GroupWise system, or connected GroupWise system by inserting asterisks (*) as wildcards in e-mail addresses.

- **Not Allowed:** Select this option to disable wildcard addressing.
- **Limited to Post Office (Default):** Select this option to limit wildcard addressing to the user's post office. This means that a user can send an item to all users on the same post office by entering * in the item's address field.
- **Limited to Domain:** Select this option to limit wildcard addressing to the user's domain. This means that a user can send an item to all users in the domain by entering *.* in the item's address field. A user can also send an item to all users on another post office in the domain by entering *.*post_office_name* in the item's address field.
- **Limited to System:** Select this option to limit wildcard addressing to the user's GroupWise system. This means that a user can send an item to all users in the GroupWise system by entering *.*.* in the item's address field. A user can also send an item to all users in another domain by entering *.*domain_name* or to all uses in another post office by entering *.*post_office_name*.
- **Unlimited:** Select this option to allow unlimited use of wildcard addressing. This means that a user can send an item to all users in another GroupWise system by entering *.*post_office_name.domain_name* or *.*domain_name* in the item's address field.

Notify Recipients

Select this option to have recipients notified when they receive an item, provided they are using GroupWise Notify. By default, this option is enabled.

Convert Attachments

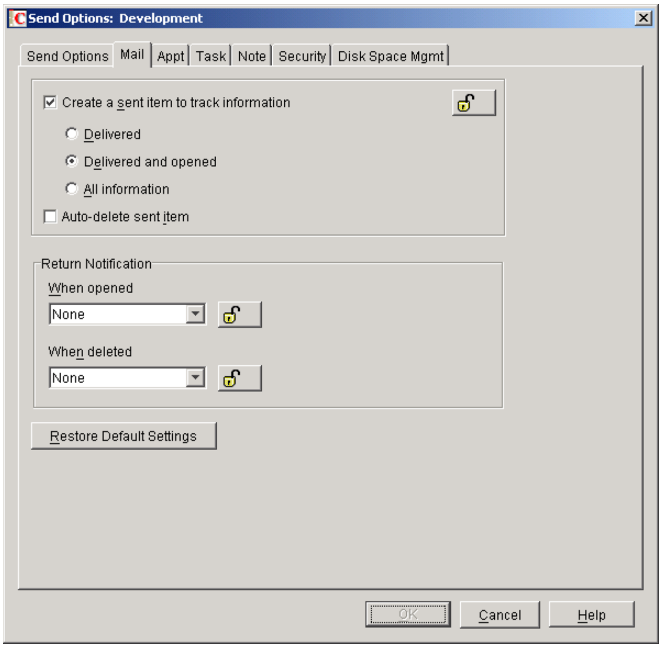
Select this option to allow conversion of attachments in items sent to non-GroupWise e-mail systems through a GroupWise gateway.

Allow Reply Rules to Loop

By default, GroupWise will not allow a rule-generated reply to be replied to by another rule-generated reply. This situation, referred to as looping, can quickly increase message traffic. To allow reply rules to loop, select this option.

Send Options: Mail

The Mail options apply to mail and phone messages only.



☑ Create a sent item to track information

○ Delivered

● Delivered and opened

○ All information

□ Auto-delete sent item

Return Notification

When opened: None

When deleted: None

Create a Sent Item to Track Information

By default, items the user sends are inserted in the user's Sent Items folder. Deselect this option if you do not want the items placed there. If items are not placed in the Sent Items folder, users cannot check the delivery status of the item. The following options are available only if this option is selected.

- **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the message to view the status.
- **Delivered and Opened (Default):** Select this option to track delivered and opened status only. The user can open the Properties window of the sent message to view the status.
- **All Information:** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the message to view the status.
- **Auto-Delete Sent Item:** Select this option to automatically delete messages from the user's Mailbox after all the recipients have deleted the messages and emptied them from the Trash.

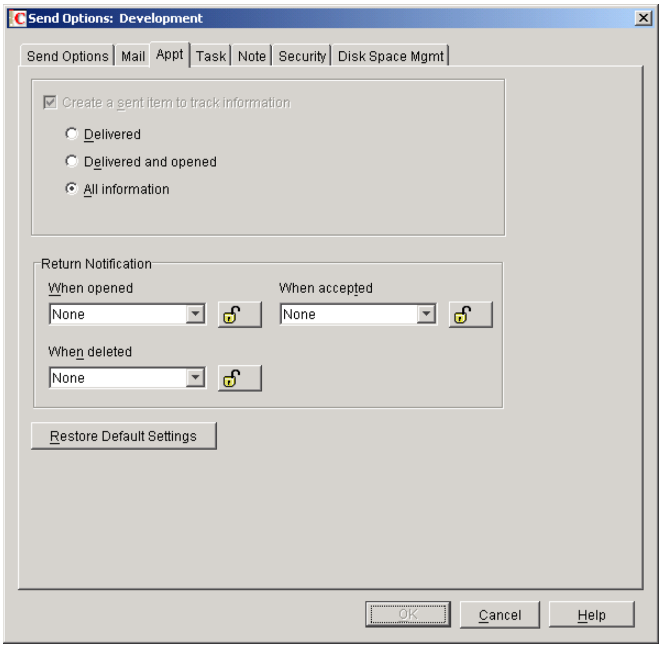
Return Notification

In addition to status tracking information, the user can receive notification when a message is opened or deleted. Choose from the following notification options:

- **None (Default):** The user will not receive notification.
- **Mail Receipt:** The user will receive a mail message stating that the recipient opened or deleted the message.
- **Notify:** The user will receive notification through GroupWise Notify when the recipient opens or deletes the message.
- **Notify and Mail:** The user will receive notification through GroupWise Notify and a mail message.

Send Options: Appointment

The Appt options apply to appointments only.



☑ Create a sent item to track information

○ Delivered

○ Delivered and opened

● All information

Return Notification

When opened: None

When accepted: None

When deleted: None

Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the Mail tab; it can only be enabled or disabled on the Mail tab. If the option is enabled, you can choose from the following status tracking levels:

- **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the appointment to view the status.
- **Delivered and Opened:** Select this option to track delivered and opened status only. The user can open the Properties window of the appointment to view the status.
- **All Information (Default):** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the appointment to view the status.

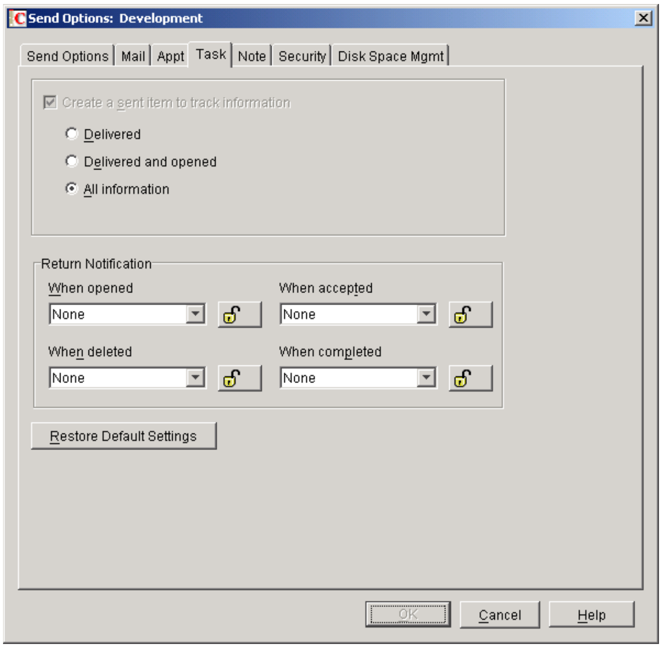
Return Notification

In addition to status tracking information, the user can receive notification when an appointment is opened, accepted, or deleted. Choose from the following notification options:

- **None (Default):** The user will not receive notification.
- **Mail Receipt:** The user will receive a mail message stating that the recipient opened, accepted, or deleted the appointment.
- **Notify:** The user will receive notification through GroupWise Notify when the recipient opens, accepts, or deletes the appointment.
- **Notify and Mail:** The user will receive notification through GroupWise Notify and a mail message.

Send Options: Task

The Task options apply to tasks only.



☑ Create a sent item to track information

○ Delivered

○ Delivered and opened

● All information

Return Notification

When opened: None

When accepted: None

When deleted: None

When completed: None

Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the Mail tab; it can only be enabled or disabled on the Mail tab. If the option is enabled, you can choose from the following status tracking levels:

- **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the task to view the status.
- **Delivered and Opened:** Select this option to track delivered and opened status only. The user can open the Properties window of the task to view the status.
- **All Information (Default):** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the task to view the status.

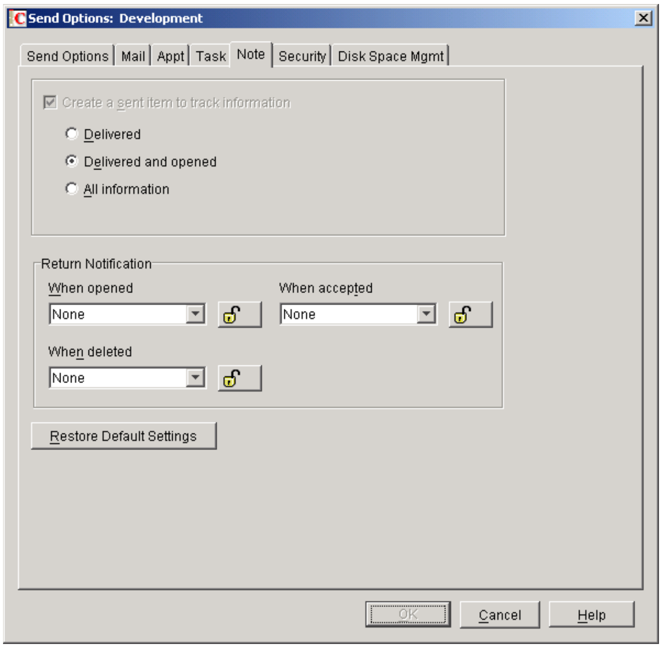
Return Notification

In addition to status tracking information, the user can receive notification when a task is opened, accepted, completed, or deleted. Choose from the following notification options:

- **None (Default):** The user will not receive notification.
- **Mail Receipt:** The user will receive a mail message stating that the recipient opened, accepted, completed, or deleted the task.
- **Notify:** The user will receive notification through GroupWise Notify when the recipient opens, accepts, completes, or deletes the task.
- **Notify and Mail:** The user will receive notification through GroupWise Notify and a mail message.

Send Options: Note

The Note options apply to notes only.



☑ Create a sent item to track information

○ Delivered

● Delivered and opened

○ All information

Return Notification

When opened: None

When accepted: None

When deleted: None

Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the Mail tab; it can only be enabled or disabled on the Mail tab. If the option is enabled, you can choose from the following status tracking levels:

- **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the note to view the status.
- **Delivered and Opened (Default):** Select this option to track delivered and opened status only. The user can open the Properties window of the note to view the status.
- **All Information:** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the note to view the status.

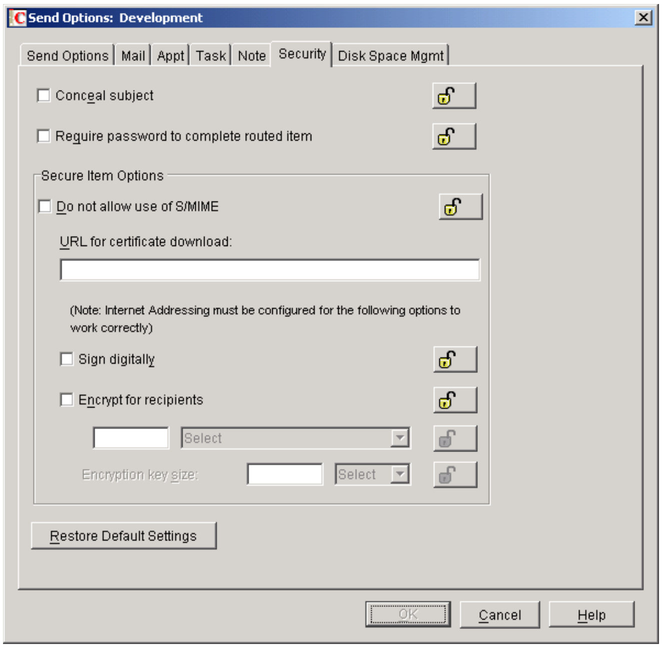
Return Notification

In addition to status tracking information, the user can receive notification when a note is opened or deleted. Choose from the following notification options:

- **None (Default):** The user will not receive notification.
- **Mail Receipt:** The user will receive a mail message stating that the recipient opened or deleted the note.
- **Notify:** The user will receive notification through GroupWise Notify when the recipient opens or deletes the note.
- **Notify and Mail:** The user will receive notification through GroupWise Notify and a mail message.

Send Options: Security

The Security options apply to all GroupWise item types (mail messages, phone messages, appointments, tasks, and notes).



□ Conceal subject

□ Require password to complete routed item

Secure Item Options

□ Do not allow use of S/MIME

URL for certificate download:

(Note: Internet Addressing must be configured for the following options to work correctly)

□ Sign digitally

□ Encrypt for recipients

Select

Encryption key size: Select

Conceal Subject

Select this option to conceal the item's subject so the notification that appears on the recipient's screen does not include the subject. The subject of the item is also concealed in the recipient's mailbox and the sender's Sent Items folder. It is visible only when the item is being read.

Require Password to Complete Routed Item

Select this option to require a user to enter a password before completing a routed item.

Secure Items Options

If users have installed security providers on their workstations, select the options you want them to use.

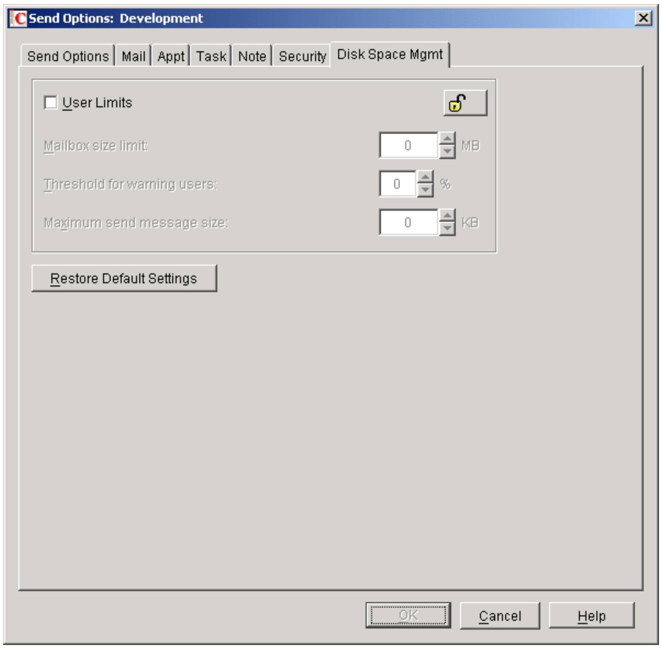
- **Do Not Allow Use of S/MIME:** Select this option to disable S/MIME functionality. This disables the Encrypt and Digitally Sign buttons (and other related S/MIME functionality) in the GroupWise client. By default, this option is enabled. When enabled, you can modify the following options.
- **URL for Certificate Download:** Specify the Internet address of your preferred certification authority. If not otherwise changed in this field, the GroupWise client accesses http://www.novell.com/groupwise/certified.html, which lists several common certification authorities.
- **Sign Digitally:** Select this option to enable users to add a digital signature to their outgoing messages. Recipients of a digitally-signed item who have S/MIME-enabled e-mail products are able to verify that the item is actually from the sender. This setting will not be a useful security measure unless you lock it as the default.

- **Encrypt for Recipients:** Select this option to enable users to encrypt an outgoing item so they can ensure that the intended recipients who have an S/MIME-enabled e-mail product are the only individuals who can read the item. This setting will not be a useful security measure unless you lock it as the default.

  If you enable the Encrypt for Recipients options, you can set the encryption algorithm and key size. The available algorithm methods (RC2, RC4, DES, 3DES) are trusted algorithms that encrypt or transform data to mask the original content. The key size sets the default size (in bits) of the encryption key that will be used with the algorithm you select. These settings will not be useful security measures unless you lock them.

Send Options: Disk Space Management

The Disk Space Management options let you enforce disk space limitations for users on a post office.



□ User Limits

Mailbox size limit: 0 MB

Threshold for warning users: 0 %

Maximum send message size: 0 KB

User Limits

Select this option if you want to impose limits on the size of users' mailboxes or the size of message they can send. By default, this option is disabled. If you enable it, modify the following options:

- **Mailbox Size Limit:** Specify the maximum amount of post office disk space available to users for storing message and attachment files. The setting uses logical disk space because attachments are shared by all recipient users on the same post office. Messages in shared folders are counted as disk space only for the owner of the shared folder. If you do not want to limit the mailbox size, set the value to zero (0).

  If users meet or exceed their mailbox size limits, they will not be able to send items until their mailboxes are under the size limit. Users can reduce the size of their mailboxes by deleting or archiving items.

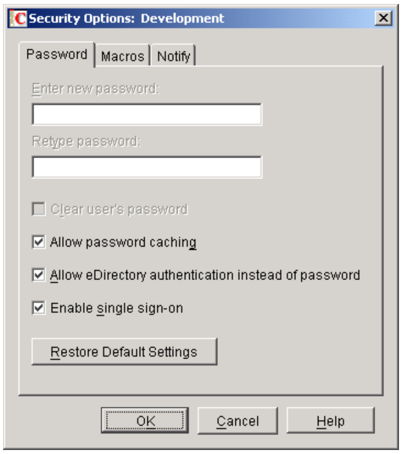
- **Threshold for Warning Users:** Select the mailbox capacity (in percentage) that must be reached before the user is warned that his or her mailbox is reaching its limit. For example, if the mailbox size limit is 200 MB and the threshold is set at 75%, users will receive warnings when their mailboxes reach 150 MB. Set the value to 0 or 100 if you do not want users to receive a warning.

- **Maximum Send Message Size:** Specify the maximum size of a message (in kilobytes) that a user can send using the GroupWise client. If the user sends an item that exceeds this size, a message notifies the user that the item is too large to send.

  You can also set message size limits at the post office level through POA configuration, at the domain level through MTA configuration, and at the GroupWise system level through Internet Agent configuration, as described in "Restricting the Size of Messages That Users Can Send" on page 175.

Modifying Security Options

1 If the Security Options dialog is not displayed, follow the instructions in "Setting Defaults for the GroupWise Client Options" on page 973 to display the dialog box.



Security Options: Development

Enter new password:

Retype password:

□ Clear user's password

☑ Allow password caching

☑ Allow eDirectory authentication instead of password

☑ Enable single sign-on

2 Click the tab that contains the options you want to change. Refer to the following sections for information about options:

"Security Options: Password" on page 997
"Security Options: Macros" on page 998
"Security Options: Notify" on page 999

NOTE: To determine which Security options are recognized by the Cross-Platform client, refer to the client options table in "Client Options Summary" on page 973.

3 If you want to prevent users from changing an option's setting, click the lock button next to it.

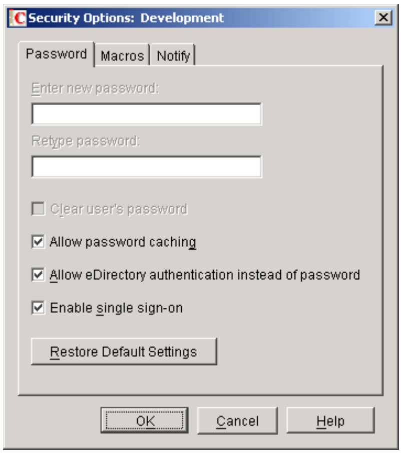
After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.

4 If you want to return all the options on a tab to their default settings, click Restore Default Settings.

5 When finished, click OK to save your changes.

Security Options: Password

The Password options let you reset a user's password and enable various methods by which a user can set up the GroupWise client so that he or she doesn't have to enter a password at startup.



Enter new password:

Retype password:

□ Clear user's password

☑ Allow password caching

☑ Allow eDirectory authentication instead of password

☑ Enable single sign-on

For background information about passwords, see Chapter 79, "GroupWise Passwords," on page 1033.

Enter New Password

This option is available only when setting client options for an individual user. You can use this option to set or reset a user's password. You should advise the user to change the password as soon as possible.

Retype Password

This option is available only when setting client options for an individual user. If you enter a new password, verify it by retyping it in this field.

Clear User Password

This option is available only when setting client options for an individual user. Select the option to clear an existing password without assigning a new password.

Allow Password Caching

Select this option to allow users to enable the Remember My Password option under Security options in the GroupWise client. The Remember My Password option stores the user's password in the workstation's Windows password list so that the user does not need to enter the password when starting GroupWise. This option is enabled by default.

The Remember My Password option applies to Windows 98 only. It will not be displayed to users running the GroupWise client on Windows NT/2000.

Allow eDirectory Authentication Instead of Password

Select this option to allow users to select the No Password Required with eDirectory option under Security options in the GroupWise client. When selected, this option lets the user access his or her mailbox without requiring a password if he or she is already logged in to Novell® eDirectory™. Mailbox access is granted based on eDirectory authentication, not on password information.

In versions of GroupWise prior to the GroupWise 5.5 Enhancement Pack, this option was called Allow NDS Single Sign-on. The option name has been changed to avoid confusion with the Novell Single Sign-on product.

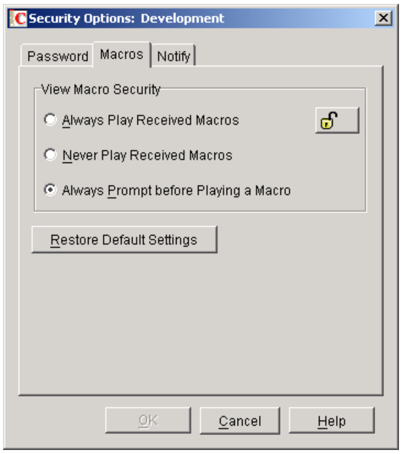
Enable Single Sign-On

Select this option to allow users to select the Use Single Sign-on option under Security Options in the GroupWise client. When selected, this option lets the user access his or her mailbox without reentering the password. The GroupWise password is stored in eDirectory for the currently logged-in user.

Novell Single Sign-on must be installed on user's workstation in order for this option to take effect.

Security Options: Macros

The Macros option determines how GroupWise handles macros that are included in received messages.



View Macro Security

○ Always Play Received Macros

○ Never Play Received Macros

● Always Prompt before Playing a Macro

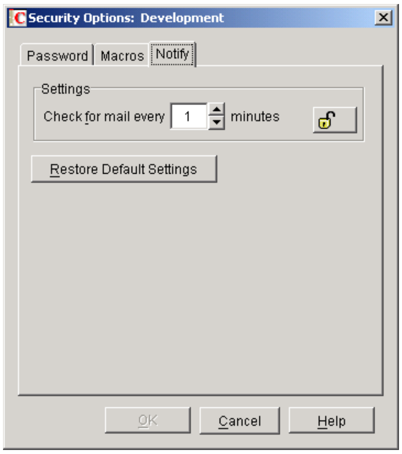
View Macro Security

Choose from the following settings to determine the level of macro security:

- **Always Play Received Macros:** Select this option to play attached macros when the message is opened.
- **Never Play Received Macros:** Select this option to ignore attached macros. Macros will not play.
- **Always Prompt Before Playing a Macro (Default):** Select this option to have the user prompted to play the macro.

Security Options: Notify

The Notify option determines how often GroupWise Notify checks a user’s mailbox for newly received items. If new items are detected, the user is notified. The default is every minute.

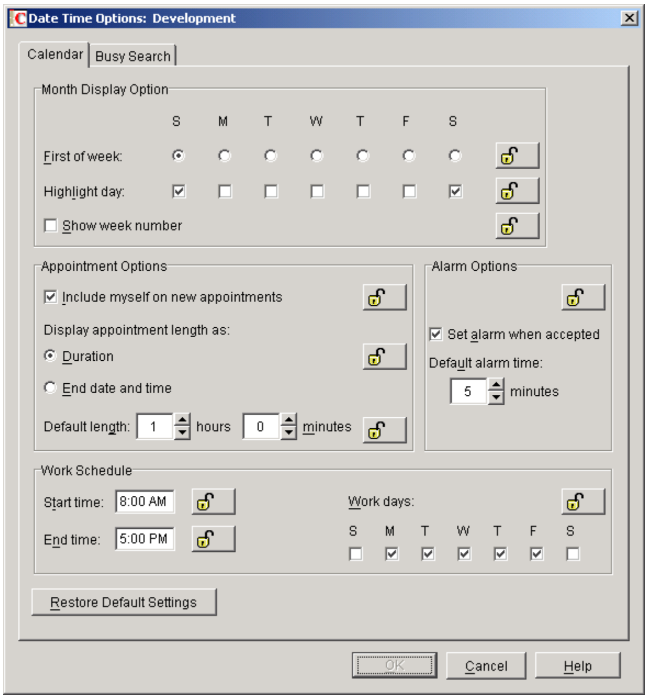


Settings

Check for mail every 1 minutes

Modifying Date and Time Options

1 If the Date and Time Options dialog box is not displayed, follow the instructions in “Setting Defaults for the GroupWise Client Options” on page 973 to display the dialog box.



Month Display Option

	S	M	T	W	T	F	S
First of week:	●	○	○	○	○	○	○
Highlight day:	☑	□	□	□	□	□	☑

□ Show week number

Appointment Options

☑ Include myself on new appointments

Display appointment length as:

● Duration

○ End date and time

Default length: 1 hours 0 minutes

Alarm Options

☑ Set alarm when accepted

Default alarm time:

5 minutes

Work Schedule

Start time: 8:00 AM

End time: 5:00 PM

Work days:

S	M	T	W	T	F	S
□	☑	☑	☑	☑	☑	□

2 Click the tab that contains the options you want to change. Refer to the following sections for information about options:

“Date and Time Options: Calendar” on page 1000

“Date and Time Options: Busy Search” on page 1002

NOTE: The Date and Time options are not currently recognized by the Cross-Platform client.

3 If you want to prevent users from changing an option's setting, click the lock button next to it.

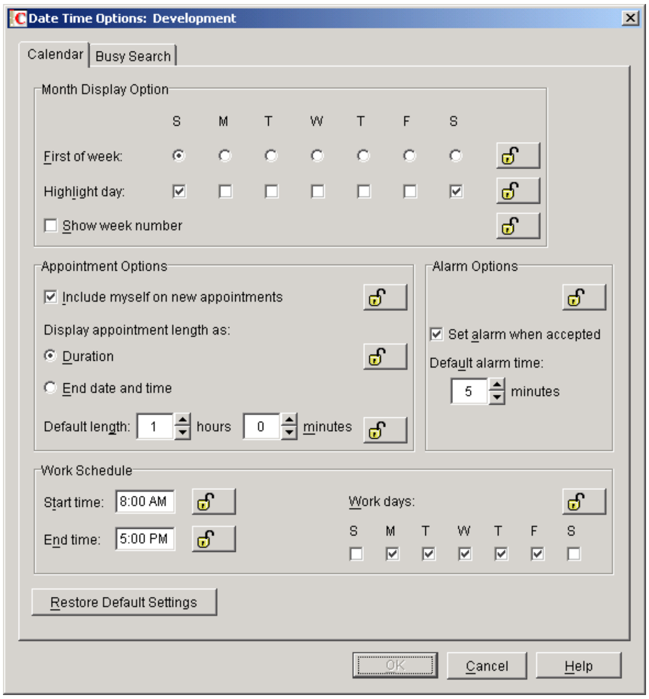
After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.

4 If you want to return all the options on a tab to their default settings, click Restore Default Settings.

5 When finished, click OK to save your changes.

Date and Time Options: Calendar

The Calendar options determine basic settings for the GroupWise Calendar.



Month Display Option

	S	M	T	W	T	F	S
First of week:	●	○	○	○	○	○	○
Highlight day:	☑	□	□	□	□	□	☑

□ Show week number

Appointment Options

☑ Include myself on new appointments

Display appointment length as:

● Duration

○ End date and time

Default length: 1 hours 0 minutes

Alarm Options

☑ Set alarm when accepted

Default alarm time: 5 minutes

Work Schedule

Start time: 8:00 AM

End time: 5:00 PM

Work days:

S	M	T	W	T	F	S
□	☑	☑	☑	☑	☑	□

Month Display Option

Select from the following options to determine how the month calendar is displayed:

- **First of Week:** Select the day of the week that you want to display as the first day on the calendar.
- **Highlight Day:** Select any days you want highlighted, such as weekends and holidays.
- **Show Week Number:** Select this option to display the week number (1 through 52) at the beginning of the calendar week.

Appointment Options

Select from the following options to determine how appointments are handled:

- **Include Myself on New Appointments:** Select this option to have the sender automatically included in the appointment's To: list. This option is enabled by default.
- **Display Appointment Length As:** When creating an appointment, the sender must specify the appointment's length. You can use this option to determine whether the sender enters a duration for the appointment or an end time for the appointment. Select the Duration setting

to have appointments display a Duration field that the sender must fill in (for example, 30 minutes, 1 hour, or 10 hours). Select the End Date and Time setting to have appointments display End Date and Time fields that the sender must fill in (for example, June 3, 2001 and 10:00 a.m.). The default setting is Duration.

- **Default Length:** Select the default length for appointments. Users can change the length. If the appointment's length is displayed as a duration, the duration defaults to this length. If it is displayed as an end date and time, the end time defaults to the start time plus the default length (for example, if the start time is 9:00 a.m. and the default length is 1 hour, the end time will default to 10:00 a.m.).

Alarm Options

Users can set appointment alarms so that they are notified prior to an appointment time. Select from the following options to determine the default settings for an alarms:

- **Set Alarm When Accepted:** Select this option to have an alarm automatically set when the user accepts an appointment. By default, this option is enabled.
- **Default Alarm Time:** Select the number of minutes before an appointment to notify the user. The default is 5 minutes.

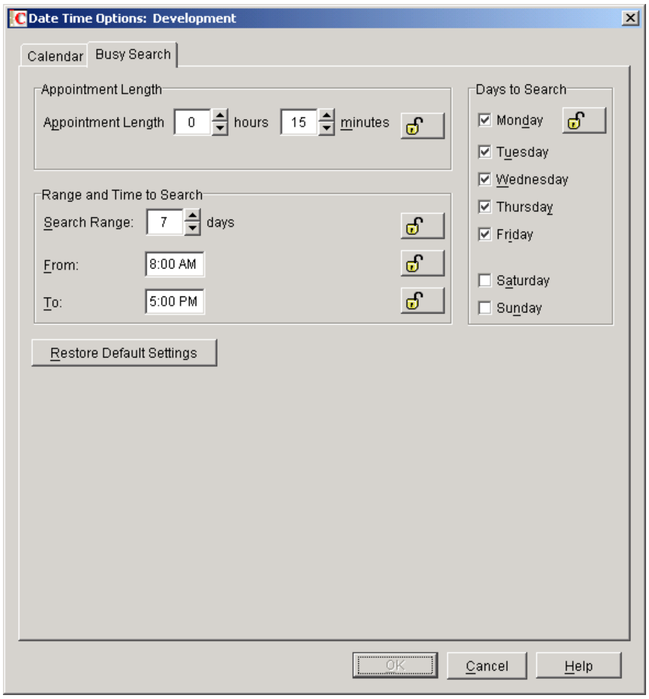
Work Schedule

The work schedule determines the user's normal work days and hours. In the calendar and during busy searches, any days or hours outside of the work schedule are represented by gray squares (Out of Office). Users can still be scheduled for appointments during non-work hours.

- **Start Time:** Select the daily start time. The default is 8:00 a.m.
- **End Time:** Select the daily end time. The default is 5:00 p.m.
- **Work Days:** Select the work days. The start time and end time will be applied to each work day.

Date and Time Options: Busy Search

The Busy Search options determine the amount of free time required for the appointment and the range of dates to search.



Appointment Length: 0 hours 15 minutes

Search Range: 7 days

From: 8:00 AM

To: 5:00 PM

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☐ Saturday
☐ Sunday

Appointment Length

Set the default appointment length to search. You can set the length in 15-minute increments. The default is 15 minutes. This setting is used only when the user does a busy search through the Busy Search option on the Tools menu. Otherwise, the default appointment length defined on the Calendar tab (see "Date and Time Options: Calendar" on page 1000) is used.

Range and Time to Search

Specify the number of days to include in the search then set the daily start and end times for the search.

Days to Search

Select the days to search. By default, the typical work days (Monday through Friday) are selected.

Resetting Client Options to Default Settings

You can reset client options to the defaults for one or more users using Mailbox/Library Maintenance.

1. In ConsoleOne, select one or more User objects (or GroupWise External Entity objects).
2. Click Tools > GroupWise Utilities > Mailbox/Library Maintenance.
3. In the GroupWise Objects list, select Users/Resources.
4. In the Actions list, select Reset Client Options > click Run.

75 Distributing the GroupWise Client

You can distribute the GroupWise® client software in various ways:

- "Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client" on page 1003
- "Using ZENworks Desktop Management to Distribute the GroupWise Windows Client" on page 1015
- "Using Red Carpet to Distribute the GroupWise Cross-Platform Client" on page 1020

Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client

During installation and subsequent updates, the GroupWise® 6.*x*. Windows client Setup program generally requires user intervention at the workstation to install the client software. By using a configuration file, you can cause installations and updates to occur, simplifying or eliminating the user response during installation. You can also use this configuration file to enable AutoUpdate, which forces updates to take place. This allows you to maintain current versions of the GroupWise software on the network.

- "Understanding the Configuration File" on page 1003
- "Installing with the Configuration File (setup.cfg)" on page 1004
- "Modifying the Configuration File" on page 1005
- "Adding LDAP Directory Service Accounts" on page 1010
- "Enabling AutoUpdate" on page 1011
- "Modifying the addon.cfg File" on page 1013
- "Error Log File" on page 1014
- "Startup Switches for Administrator-Defined Setup" on page 1014

NOTE: This section does not apply to the Cross-Platform client.

Understanding the Configuration File

The use of a configuration file to install GroupWise is often called an administrator-defined setup. The configuration file, setup.cfg, is an ASCII text file that supports extended ASCII characters. The file contains the responses normally provided by the user during the installation of the Windows client files; for example, the path for the client files, whether to complete a workstation or standard installation, and the folder for the GroupWise icon are specified in this file. Information can be added to the configuration file to add predefined LDAP directory service accounts to the Address Book in the client during installation.

When the GroupWise Windows client setup.exe file is executed, it looks in the same directory for a setup.cfg file. If none is found, the installation proceeds, prompting the user for the needed information. If the setup.cfg file is found, the setup program installs the software, using the information outlined in the configuration file. Depending on the entries in the configuration file, the user might or might not be prompted to provide information during the installation.

If you are going to use a configuration file to install Windows client software, users should be given Read and File Scan rights to the *software_distribution_directory*\client and *software_distribution_directory*\client\win32 directories. (This does not apply if you are running AutoUpdate over an IP connection.)

Installing with the Configuration File (setup.cfg)

During the installation of GroupWise Administration, the GroupWise client files were copied to the software distribution directory on your server. For example, if you accepted the default z:\grpwise\software as your target, the GroupWise client software was copied to z:\grpwise\software\client\win32.

Installing with a Configuration File (setup.cfg)

1. Make a backup copy of *software_distribution_directory*\client\setup.cfg. Using an ASCII text editor, edit the setup.cfg file entries with the values you want. See "Modifying the Configuration File" on page 1005 for more information.
2. If you want to add predefined LDAP directory service accounts to the Address Book, follow the procedure in "Adding LDAP Directory Service Accounts" on page 1010.
3. If you want to use AutoUpdate, follow the procedure in "Enabling AutoUpdate" on page 1011.
4. Save setup.cfg > copy the file to the *software_distribution_directory*\client\win32 directory.
5. If you want to install additional components on users' workstations, follow the procedure in "Modifying the addon.cfg File" on page 1013.

   For information about installing GroupWise Messenger as an additional component by modifying the addon.cfg file, see "Installing the Messenger Windows Client as a GroupWise Windows Client Add-On" in "Managing Messenger Client Users" in the *Messenger 1.0 Administration Guide*.

If you use several different configuration files, you will need to save them with different names and use the config=*setup filename* startup switch. See "Startup Switches for Administrator-Defined Setup" on page 1014 for more information.

To stop setup.exe from using the setup.cfg file, delete setup.cfg from the directory where setup.exe resides.

Setupip.fil File

In previous versions of GroupWise, all language versions of the setupip.fil file, used when running AutoUpdate over an IP connection, were not included on the CD and had to be downloaded from the Novell® Downloads page (http://download.novell.com).

In GroupWise 6.5 Support Pack 1, all non-localized files are included in the setupip.fil file and there is a separate setupip.*language_code* file for each language (setupip.de, setupip.fr, and so on). All of these files are included in the setupip directory on the *GroupWise 6.5 Client* CD in Support Pack 1 and do not need to be downloaded separately.

If you did not select all options for Client when you initially created your software distribution directory, you will need to copy the setupip directory from the *GroupWise 6.5 Client* CD to the software distribution directory. Copy the setupip.fil file and any language-specific setupip.*language_code* files you want to the HTTP Web server that you will be using for SetupIP. If there are multiple SetupIP files on the Web server, users are prompted for which languages they want to install. For more information, see "Enabling AutoUpdate" on page 1011.

Modifying the Configuration File

The configuration file is divided into the following sections. In the configuration file, each section head must be enclosed in brackets [ ] as shown.

- "[GroupWiseSetup]" on page 1005
- "[ShowDialogs]" on page 1006
- "[AutoUpdate]" on page 1007
- "[Startup]" on page 1008
- "[GWTIP]" on page 1008
- "[GWMAILTO]" on page 1009
- "[GWCHECK]" on page 1009
- "[IntegrationApps]" on page 1010
- "[Languages]" on page 1010

[GroupWiseSetup]

- "Version=" on page 1005
- "StandardInstall=" on page 1005
- "Path=" on page 1005
- "Folder=" on page 1006
- "LaunchMessenger=" on page 1006
- "DefaultIPAddress=" on page 1006
- "DefaultIPPort=" on page 1006

Version=

This must match the version being installed; otherwise, the setup program will not use setup.cfg. The default is 6.

StandardInstall=

Specify the type of installation desired. Specify No for a workstation installation, which allows the user to run GroupWise from the network. Specify Yes for a standard installation, which allows the user to run GroupWise from the computer's hard drive. A standard installation is required to use Caching mode and Remote mode. The default is No.

Path=

This is the path where you want GroupWise to be installed during a standard installation. The default path is c:\novell\groupwise\.

Folder=

This will create and install the GroupWise icons to the specified folder. The default folder is GroupWise.

LaunchMessenger=

This optional entry specifies whether GroupWise Notify should be launched when GroupWise starts.

DefaultIPAddress=

This optional entry specifies the default IP address for the client to use the first time it is started.

DefaultIPPort=

This optional entry specifies the default IP port for the client to use the first time it is started.

[ShowDialogs]

HideAllDialogs=

Specify No to display dialog boxes during the installation. Specify Yes to hide the dialog boxes. A progress indicator will be displayed to inform the user of the installation status. The default is No.

If an entry is missing from the setup.cfg file and HideAllDialogs=Yes, the setup program will select the default setting. If HideAllDialogs=No, the setup program will prompt the user for a selection.

Welcome=

Specify Yes to display the Welcome dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

SetupOptions=

Specify Yes to display the Setup Options dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

DestinationDirectory=

Specify Yes to display the Destination Directory dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

SelectOptionalComponents=

Specify Yes to display the Select Optional Components dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

SelectProgramFolder=

Specify Yes to display the Select Program Folder dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

SelectStartUpFolderSoftware=

Specify Yes to display the Select Startup Folder Software dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

LanguageSelection=

Specify Yes to display the Language Selection dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

SoftwareIntegrations=

Specify Yes to display the Software Integrations dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

StartCopyingFiles=

Specify Yes to display the Start Copying Files dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

SetupComplete=

Specify Yes to display the Setup Complete dialog box during the installation. Specify No to hide this dialog box. The default is Yes.

[AutoUpdate]

When an update to the GroupWise software is available, users are prompted if they want to install the new software when they start GroupWise. For complete instructions on enabling AutoUpdate, see "Enabling AutoUpdate" on page 1011.

- "Enabled=" on page 1007
- "SetupIPEnabled=" on page 1008
- "ForceUpdate=" on page 1008
- "GraceLoginCount=" on page 1008
- "PromptUntilUpdated=" on page 1008

Enabled=

Specify Yes if you want users to be prompted to update their GroupWise client software as soon as a newer version is available. Specify No if you want to disable the AutoUpdate feature. The

ForceUpdate= entry is then ignored. This can be useful if you intend to distribute the client software using a different method such as ZENworks® Application Launcher, or if you want to disable AutoUpdates at the post office level during a migration to a newer version of GroupWise. The default is Yes.

SetupIPEnabled=

The default is No. Specify Yes if you want to run AutoUpdate over an IP connection to a software distribution directory that resides on an HTTP web server.

ForceUpdate=

When this entry is set to Yes, GroupWise automatically updates the users' software. The default is No.

Users can still click Cancel to cancel out of the update; however, they cannot run the client software and access their mailboxes until they update the software.

GraceLoginCount=

Specify the number of grace logins allowed before you will require the users to update their client software. If ForceUpdate is set to No, this entry is ignored.

PromptUntilUpdated=

When PromptUntilUpdated= is set to Yes, the user will be prompted to update the client each time the GroupWise client starts. The user can choose not to install the new software when prompted and still run the currently installed version of the client. The AutoUpdate reminder will appear the next time the user starts the client. The default is No.

[Startup]

Notify=

If you specify Yes, the setup program will place Notify in the Startup folder to be started automatically when the computer starts. The default is No.

[GWTIP]

The Tip of the Day introduces what's new in the GroupWise client, as well as displaying a variety of hints about using GroupWise. A new tip is displayed each time GroupWise is started.

- "Default=" on page 1008
- "Hide=" on page 1008
- "Workstation=" on page 1009

Default=

If you specify No, Tip of the Day will not be installed. If you specify Yes, Tip of the Day will be installed. The default is Yes.

Hide=

If you specify No, Tip of the Day will appear in the Select Components dialog box. The default is No.

The Hide= entry allows the system administrator to force the user to install or not install a particular component. If Hide=Yes, then the component will not be listed in the Select Components dialog and the Default= entry will determine if the component is going to be installed. For example, if Hide=Yes and Default=Yes, then the component will always be installed. However, if Hide=Yes and Default=No, then the component will never be installed.

Workstation=

If you specify No, Tip of the Day will not be available for a workstation installation. If you specify Yes, Tip of the Day will be available for a workstation installation. The default is Yes.

[GWMAILTO]

This section enables Internet Browser Mail Integration, which makes the GroupWise client the default e-mail program in the user's browser. Whenever a user clicks an e-mail link on a Web page or chooses Mail in the browser, the GroupWise client opens.

- "Default=" on page 1009
- "Hide=" on page 1009
- "Workstation=" on page 1009

Default=

If you specify No, Internet Browser Mail Integration will not be installed. If you specify Yes, Internet Browser Mail Integration will be installed. The default is Yes.

Hide=

If you specify No, Internet Browser Mail Integration will appear in the Select Components dialog box. The default is No.

The Hide= entry allows the system administrator to force the user to install or not install a particular component. If Hide=Yes, then the component will not be listed in the Select Components dialog and the Default= entry will determine if the component is going to be installed. For example, if Hide=Yes and Default=Yes, then the component will always be installed. However, if Hide=Yes and Default=No, then the component will never be installed.

Workstation=

If you specify No, Internet Browser Mail Integration will not be available for a workstation installation. If you specify Yes, Internet Browser Mail Integration will be available for a workstation installation. The default is Yes.

[GWCHECK]

This section installs and enables GroupWise Check (also called GWCheck). GroupWise Check is a tool that performs maintenance and repair tasks to keep GroupWise operating efficiently. It is essentially a standalone version of the Mailbox/Library Maintenance feature available in GroupWise Administration in ConsoleOne. GWCheck will check and repair GroupWise user, message, library, and resource databases without having ConsoleOne® and the GroupWise snap-in loaded. In addition to checking post office, user, and library databases, it will also check remote and archive databases.

- "InstallGWCheck=" on page 1010
- "GWCheckEnabled=" on page 1010

InstallGWCheck=

Specify Yes to install GWCheck files to the workstation. Specify No to not install GWCheck. The default is Yes.

GWCheckEnabled=

Specify Yes to install the files to the same directory as the GroupWise client, which will result in the Repair Mailbox option being enabled under the Tools menu in the client. Specify No to install the files in a GWCheck subdirectory below the GroupWise client directory, which disables the Repair Mailbox option until the files are manually copied into the GroupWise directory. The default is No.

[IntegrationApps]

GroupWise will install integration for the following applications, if found, unless the entry is set to No.

- Lotus Word Pro
- Microsoft Binder
- Microsoft Excel (versions higher than 7.0)
- Microsoft Excel 7.0
- Microsoft Word (versions higher than 7.0)
- Microsoft Word 7.0
- Microsoft PowerPoint
- Corel Presentations
- Corel Quattro Pro
- Corel WordPerfect 7.0
- Corel WordPerfect 8.0
- Corel WordPerfect 9.0
- Corel WordPerfect 10.0

[Languages]

The default language is set to English, and all other languages are set to No, meaning they will not be installed. See the setup.cfg file for a listing of the different languages. The GroupWise client might not yet be available in all listed languages.

Adding LDAP Directory Service Accounts

LDAP directory service accounts provide users with the ability to search directory services such as Bigfoot* for names of people. Each search can check potentially millions of names. After locating a name through a directory service search, users can add those names to their personal address books.

You can add predefined LDAP directory service accounts to the Address Book by adding information to setup.cfg. This information can be added even after the initial installation. After the accounts are added, this information does not have to be removed from setup.cfg. During subsequent installations, GroupWise will add any new accounts listed but will not update or duplicate existing LDAP accounts.

The user can also choose to add LDAP directory service accounts after the GroupWise client is installed.

To add an LDAP account during installation, add the following lines to the setup.cfg file, providing information that is specific to the account:

```
[LDAP Account 1]
Description=Ldap Server1
Server=ldap.server1.com
Port=389
SearchRoot=c=us
Login=TRUE
```

You can add multiple accounts:

```
[LDAP Account 2]
Description=Ldap Server2
Server=ldap.server2.com
Port=389
SearchRoot=0=widget, c=us
Login=FALSE
```

Parameter	Description
Description=	The name that displays in the list of LDAP directory services in the Address Book.
Server=	The LDAP server name or IP address.
Port=	The LDAP directory service's port number. The number is usually 389.
SearchRoot=	The base or root of the LDAP directory service where the user will search for names. For example, the base could be a country, organization, or other type of grouping. This is not required for all LDAP directory services. If a search root is required, the LDAP directory service will provide the information.
Login=	TRUE means users are prompted for a username and password when they use that LDAP directory service.

Enabling AutoUpdate

AutoUpdate can occur whether users have a mapped drive or IP connection to the software distribution directory. If users have a mapped drive to the software distribution directory, make sure they have Read and Scan rights to the *software_distribution_directory*\client and *software_distribution_directory*\client\win32 directories.

IMPORTANT: To install the GroupWise client using AutoUpdate, you must first make sure GroupWise 6.*x* Administration and GroupWise 6.*x* agents have been installed, and that administration, agent, and client software has been updated.

IMPORTANT: If you did not select all options for Client when you initially created your software distribution directory, you will need to copy the setupip directory from the *GroupWise 6.5 Client* CD to the software distribution directory. If you are going to use AutoUpdate over an IP connection, copy setupip\setupip.fil to an HTTP web server, or copy the entire client directory to the HTTP web server.

For information about the location of setupip.fil, see "Setupip.fil File" on page 1004.

In the following procedure, steps 1-4 apply only if you will be using an IP connection for AutoUpdate.

1 Run *software_distribution_directory*\setupip\writeip.exe.

Specify an IP location for setupip.fil (or the IP location of the software distribution client subdirectory). For example, you can specify:

```
http://151.155.135.122/gw65/client
```

or

```
http://intranet.company.com/software/gw65/gwclient
```

You can include proxy and port information, for example:

```
http://name.mycompany.com/software/gw65/
client;proxy.place.mycompany:1690
```

You can specify up to five locations. During AutoUpdate, each location is checked, in order, until a connection is made.

If you select Choose IP Address at Random, the order in which the locations are checked is selected randomly when AutoUpdate occurs. This will balance the load on the web server.

2 Specify other options, such as the location for downloading the client installation files (setupip.fil or the client subdirectory files).

You can have files downloaded to a temporary or specific directory.

If you select Allow the User to Change the Download Directory, the user is prompted for the location of the download directory and can change the default location.

3 Click OK.

The setupip.exe file is created. The writeip.ini file is also created, which stores the options you selected in writeip.exe.

4 Copy setupip.exe to the *software_distribution_directory*\client\win32 directory.

5 Make a backup copy of *software_distribution_directory*\client\setup.cfg.

6 Using an ASCII text editor, edit the setup.cfg file entries with the values you want.

6a Under the [AutoUpdate] heading, specify

```
Enabled=Yes
```

6b Specify

```
ForceUpdate=Yes
```

if you want GroupWise to automatically update the users' client software

or

```
ForceUpdate=No
```

if you want users to be prompted to update their client software.

6c Specify the number of grace logins you want to allow a user before forcing an AutoUpdate, for example:

```
GraceLoginCount=2
```

This entry is ignored if ForceUpdate=No.

6d If you will be using an IP connection for AutoUpdate, specify

```
SetupIPEnabled=Yes
```

7. Save the file as setup.cfg. Copy setup.cfg from *software_distribution_directory*\client to *software_distribution_directory*\client\win32.

8. If necessary, modify addon.cfg files with the values you want. See "Modifying the addon.cfg File" on page 1013 for more information.

9. Log in to ConsoleOne as an Admin equivalent.

10. Click Tools > GroupWise System Operations.

11. Double-click Software Directory Management.

12. Click the software distribution directory > Update.

13. Select Force Auto-Update Check by GroupWise Components.

    This causes the GroupWise client to check for a new version. If a new version is found, the next time a user starts the GroupWise client, he or she is prompted to update the client software. If you have set ForceUpdate=Yes, the user will not be prompted before installation begins. If a mapped drive to the software distribution directory is found, the client software is installed from the mapped drive. If a mapped drive to the software distribution directory is not found, GroupWise looks at the IP locations you specified in writeip.ini and installs the client software.

    In the event that no connection to the software distribution directory can be made, the file setupip.err is created in c:\windows of the user's workstation. This file explains why none of the connections could be made.

Modifying the addon.cfg File

The addon.cfg file is an ASCII text file that supports extended ASCII characters. The GroupWise client setup program uses the addon.cfg file to install additional components on users' workstations. The components might include software not shipped with GroupWise. The addon.cfg is specific to each program being installed. The required program files and the associated addon.cfg file must be copied to a subdirectory under *software_distribution_directory*\client\win32\addons.

During the client installation, the GroupWise setup program will search the subdirectories under the \addons directory for any addon.cfg files. The setup program will then execute the installation program for that component using the settings specified in the addon.cfg. If an entry is missing in the addon.cfg file, the installation program will prompt the user for the required information.

The addon.cfg files for Internet Browser Mail Integration and GroupWise Tip of the Day are included in the corresponding subdirectories under \addons, but the basic control for installing these two components is in the [GWMAILTO] and [GWCHECK] sections of setup.cfg.

For information about installing GroupWise Messenger as an additional component by modifying the addon.cfg file, see "Installing the Messenger Windows Client as a GroupWise Windows Client Add-On" in "Managing Messenger Client Users" in the *Messenger 1.0 Administration Guide*.

When creating an addon.cfg file for a different component, you must include at least the following section headings and associated entries. If the installation program requires additional information, you can include that information as additional entries. The required entries are as follows:

- "[GroupWiseAddon]" on page 1014
- "[Name]" on page 1014
- "[Description]" on page 1014

[GroupWiseAddon]

This section head must be included with the following entries.

Entry	Example
Install=*add-on's_setup_program_filename*	`Install=setup.exe`
Parameters=*parameters_to_be_passed_on_to_the_add-on's_setup_program*	`Parameters=/install`
Silent=*parameters_to_append_to_administrator-defined_setup*	`Silent=/s`
Size=*installed_size_of_add-on_in_kilobytes*	`Size=100`

[Name]

Under this section head, specify the two-letter language code for the language being installed, followed by the name of the add-on. This name appears in the components listing.

Example: `US=GroupWise Tip of the Day`

[Description]

Under this section head, specify the two-letter language code followed by a short description of the add-on. This description appears in the Description field when the component is highlighted in the component listing.

Example: `US=GroupWise Tip of the Day introduces new features and provides tips for using the GroupWise client.`

Error Log File

If an error occurs during the installation and ShowDialogs=No, the error message is logged in gwsetup.err in the user's \windows directory. If ErrorMessage=*error_text* has been added as the last entry under the [GroupWiseSetup] section, the error text will be displayed. Otherwise, a generic error message will be displayed notifying the user to contact the system administrator. The log file is an ASCII text file.

Startup Switches for Administrator-Defined Setup

The following startup switches can be used in conjunction with an administrator-defined setup. These switches can be used individually or in combination.

- config=setup_filename
- noconfig
- record

config=*setup_filename*

This runs the setup program using a configuration file other than setup.cfg. The other configuration file must be located in the software distribution directory. This switch does not apply when the GroupWise Windows client setup program is executed by AutoUpdate.

Syntax: `config=`*`setup_filename`*

Example: `setup config=test.cfg`

noconfig

This runs the setup without using the configuration file, even if one exists.

Syntax: `noconfig`

Example: `setup noconfig`

record

This option runs the setup program, displaying all installation dialog boxes, and records the installation responses as they are selected. No installation files are copied and no changes are made to your workstation. After setup finishes, a corresponding setup.cfg file is created in the \windows directory of your workstation.

Syntax: `record`

Example: `setup record`

Using ZENworks Desktop Management to Distribute the GroupWise Windows Client

You can use the Application Management functionality in Novell® ZENworks® Desktop Management to distribute the GroupWise Windows client to workstations. The following sections provide instructions:

- "Understanding the GroupWise Windows Client .aot Files" on page 1015
- "Creating a GroupWise Client Application Object" on page 1016

IMPORTANT: This information assumes that you are familiar with ZENworks Desktop Management. For background information, or for help completing the ZENworks tasks outlined in the steps below, see the ZENworks Desktop Management documentation at the Novell ZENworks documentation site (http://www.novell.com/documentation-index/index.jsp?category=ZENworks).

Understanding the GroupWise Windows Client .aot Files

The most effective way to create a GroupWise client Application object is from an Application Object Template (.aot) file. If desired, you can use the ZENworks Desktop Management snAppShot™ utility to create a GroupWise Windows client .aot file, or you can use one of the predefined .aot files included with GroupWise:

- **us-9x.aot:** Creates an Application object you can use to install the English version of the GroupWise client to a Windows 95/98/ME workstation.
- **us-9xwms.aot:** Creates an Application object you can use to install the English version of the GroupWise client and the Windows Messaging System to a Windows 95/98/ME workstation
- **us-nt.aot:** Creates an Application object you can use to install the English version of the GroupWise client to a Windows NT/2000/XP workstation.
- **us-ntwms.aot:** Creates an Application object you can use to install the English version of the GroupWise client and the Windows Messaging System to a Windows NT/2000/XP workstation.

- **multi19x.aot:** Creates an Application object you can use to install the English, Portuguese, French, Italian, German, Spanish, Danish, Dutch, Norwegian, Finnish, and Swedish versions of the GroupWise client to a Windows 95/98/ME workstation.
- **multi1nt.aot:** Creates an Application object you can use to install the English, Portuguese, French, Italian, German, Spanish, Danish, Dutch, Norwegian, Finnish, and Swedish versions of the GroupWise client to a Windows NT/2000/XP workstation.
- **multi29x.aot:** Creates an Application object you can use to install the English, Hungarian, Czech, Polish, and Russian versions of the GroupWise client to a Windows 95/98/ME workstation.
- **multi2nt.aot:** Creates an Application object you can use to install the English, Hungarian, Czech, Polish, and Russian versions of the GroupWise client to a Windows NT/2000/XP workstation.
- **multi39x.aot:** Creates an Application object you can use to install the English, Chinese Simplified, Chinese Traditional, Japanese, and Korean versions of the GroupWise client to a Windows 95/98/ME workstation.
- **multi3nt.aot:** Creates an Application object you can use to install the English, Chinese Simplified, Chinese Traditional, Japanese, and Korean versions of the GroupWise client to a Windows NT/2000/XP workstation.

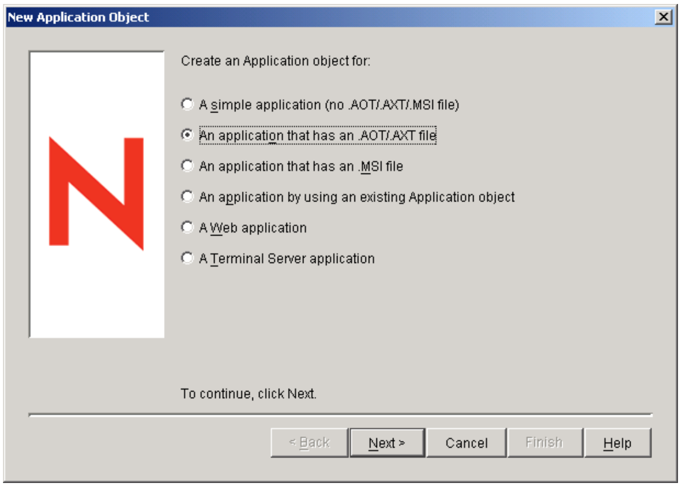
The .aot files contain the basic information required to create GroupWise client Application objects in Novell eDirectory®. For example, the multi2nt.aot file can be used to create an Application object that, when associated with users, will cause the English, Czech, Hungarian, Polish, and Russian versions of the GroupWise client to be installed to a user's Windows NT/2000/XP workstation. For this to work, you must have already installed the files for these language versions to a GroupWise software distribution directory or another installation source directory.

Creating a GroupWise Client Application Object

The following steps explain how to use ZENworks Desktop Management to create an GroupWise client Application object from one of the .aot files. Depending on your version of ZENworks Desktop Management, the steps you need to complete might be slightly different.

1 In ConsoleOne®, right-click the container where you want to create the GroupWise client Application object, then click New > Object to display the New Object dialog box.

2 In the list of objects, click App:Application > OK to display the New Application dialog box.



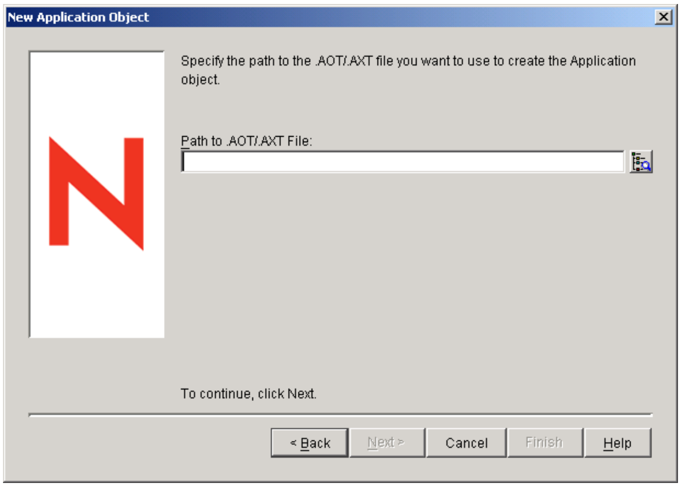
New Application Object

Create an Application object for:

○ A simple application (no .AOT/.AXT/.MSI file)
● An application that has an .AOT/.AXT file
○ An application that has an .MSI file
○ An application by using an existing Application object
○ A Web application
○ A Terminal Server application

To continue, click Next.

3 Select the An Application that Has an .AOT/.AXT File option, then click Next to display the .AOT/.AXT file path page.



New Application Object

Specify the path to the .AOT/.AXT file you want to use to create the Application object.

Path to .AOT/.AXT File:

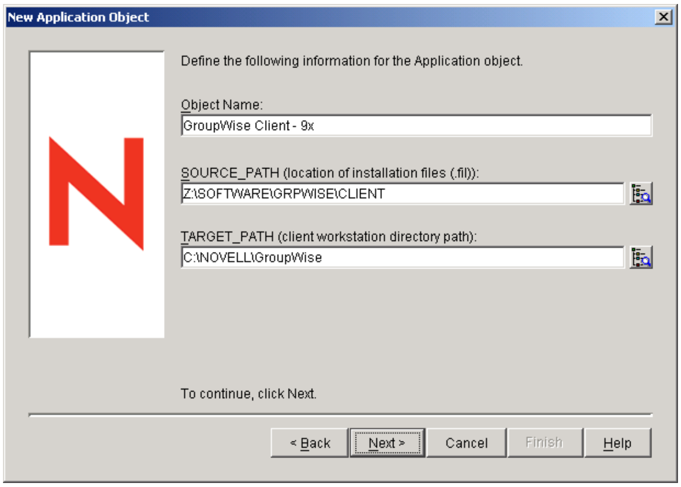
To continue, click Next.

4 In the Path to .AOT/.AXT File field, browse for and select the .aot file you want to use.

By default, the .aot files are located in the client\zen directory in the GroupWise software distribution directory or on the *GroupWise 6.5 Client* CD

For example, if you want to create an Application object that will install the English, Czech, Hungarian, Polish, and Russian versions of the GroupWise client to a Windows NT/2000/XP workstation, select the multi2nt.aot file.

5 Click Next to display the Application object information page, then customize the object name, source path, and target path information if necessary.



New Application Object

Define the following information for the Application object.

Object Name: GroupWise Client - 9x

SOURCE_PATH (location of installation files (.fil)): Z:\SOFTWARE\GRPWISE\CLIENT

TARGET_PATH (client workstation directory path): C:\NOVELL\GroupWise

To continue, click Next.

Object Name: This is the name that will be used for the Application object in eDirectory. You might want to use a descriptive name (for example, "GroupWise ECHPR Client - Windows9x" for the English, Czech, Hungarian, Polish, and Russian versions installed to a Windows 95/98/ME workstation.

SOURCE_PATH: This is the directory from which the GroupWise client will be installed. Specify the full path to the client directory (for example,

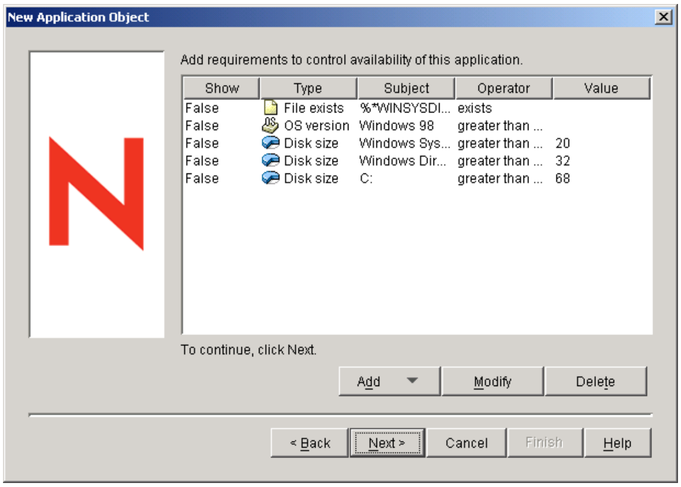
\\server1\vol1\grpwise\software\client). Unless all users will have the same drive mapping to the volume, make sure you use a UNC path.

This path is saved as the SOURCE_PATH variable. If you need to change it later, you can do so on the Application object's Macros page (Application object > Common tab > Macros page).

TARGET_PATH: This is the workstation directory where the GroupWise client will be installed. Specify a path relative to the user's workstation.

This path is saved as the TARGET_PATH variable. If you need to change it later, you can do so on the Application object's Macros page (Application object > Common tab > Macros page).

6 Click Next to display the system requirements page, then modify the system requirements if necessary.

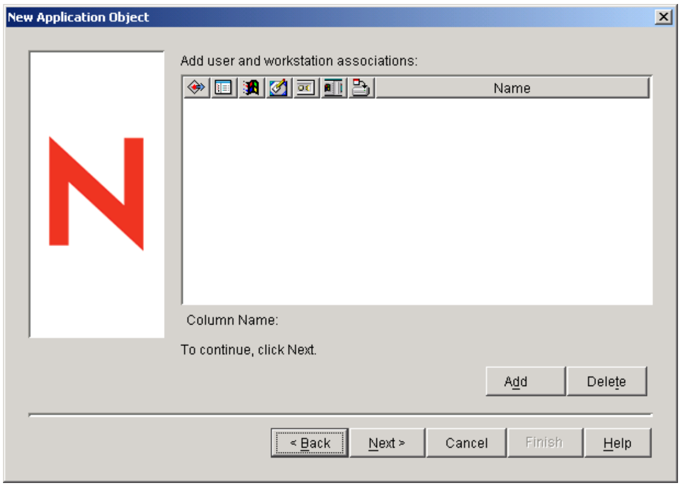


Add requirements to control availability of this application.

Show	Type	Subject	Operator	Value
False	File exists	%*WINSYSDI...	exists	
False	OS version	Windows 98	greater than ...	
False	Disk size	Windows Sys...	greater than ...	20
False	Disk size	Windows Dir...	greater than ...	32
False	Disk size	C:	greater than ...	68

To continue, click Next.

7 Click Next to display the user associations page.



Add user and workstation associations:

Column Name:

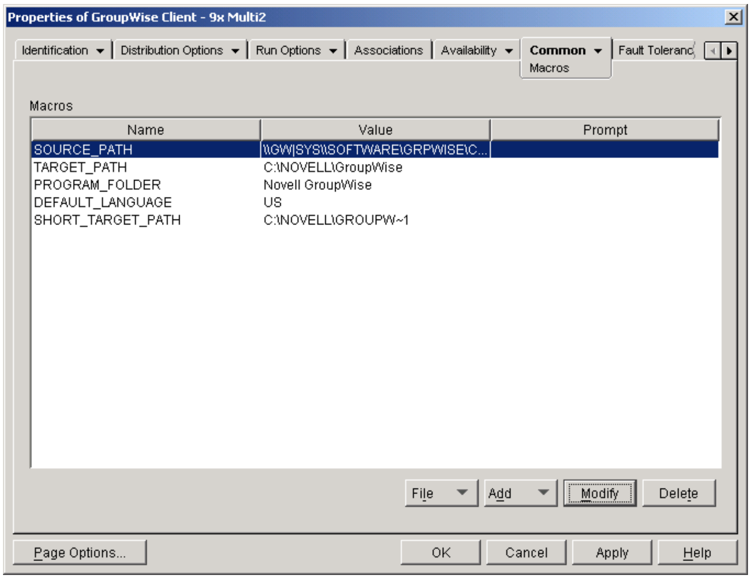
To continue, click Next.

You can associate the Application object with the users and workstations you want it distributed to at this time, or you can create the associations later.

8 After you've added the associations you want, click Next, review the information, then click Finish to create the Application object.

9 Right-click the newly-created GroupWise client Application object, then click Properties.

10 Click Common > Macros to display the Macros page.



Name	Value	Prompt
SOURCE_PATH	\\GW|SYS\\SOFTWARE\GRPWISE\C...	
TARGET_PATH	C:\NOVELL\GroupWise	
PROGRAM_FOLDER	Novell GroupWise	
DEFAULT_LANGUAGE	US	
SHORT_TARGET_PATH	C:\NOVELL\GROUPW~1	

If you used one of the multi*x*.aot files to create the Application object, the Macros list includes a DEFAULT_LANGUAGE variable. This variable specifies the interface language that the GroupWise client will default to when it is installed. If necessary, individual users can change the language when they start the GroupWise client. If you modify the default language, use the language codes listed under "/l-xx" on page 1027.

If you have users who use different language versions and you don't want them to need to change the default language, you can use the same .aot file to create multiple Application objects. For each Application object, you would need to specify a default language and then associate the Application object with the users who would want that default language.

11 Configure any other Application object settings required to provide the performance or functionality you want.

For example, you can configure the Application object so that the GroupWise client will be installed immediately upon distribution to the user's workstation, without any intervention by the user. Or, you can change the locations where the GroupWise client's icon will be displayed. For information about Application object settings, see the ZENworks Desktop Management documentation at the Novell Documentation Web site (http://www.novell.com/documentation-index/index.jsp?category=ZENworks).

After you associate the Application objects with the users you want, Novell Application Launcher will display the Application object's icon on the users' workstations, provided the workstation meets the operating system requirements. If the Application object's icon does not appear immediately, have the user refresh Novell Application Launcher.

12 If necessary, repeat the above steps to create additional GroupWise client Application objects from the GroupWise client .aot files.

Using Red Carpet to Distribute the GroupWise Cross-Platform Client

You can install the GroupWise Cross-Platform client and agents using Red Carpet™ 2.0 or later. Refer to the Red Carpet Web site (http://www.ximian.com/products/redcarpet) for additional information.

76 Supporting the GroupWise Client in Multiple Languages

The GroupWise client software is available in a broad range of languages to meet the needs of users in many countries. If your GroupWise system services users who speak more than one language, the following tasks help you meet your multilingual users' needs.

- "Providing the GroupWise Client Software in Multiple Languages" on page 1021
- "Providing Post Office Support for Multiple Languages" on page 1021

Providing the GroupWise Client Software in Multiple Languages

1. Make sure that you have the multilingual version of GroupWise.

   Both initial releases and Support Packs are provided in an English Only version (for faster download) and a multilingual version (that includes all available languages).

2. Install the client software in the languages you need in one or more software distribution directories, following the instructions in "Software Directory Management" on page 57.
3. Distribute the client software to users, as described in Chapter 75, "Distributing the GroupWise Client," on page 1003.

By installing the GroupWise client software in their language of choice, users can begin using GroupWise in that language immediately. However, there are a few language-related details of GroupWise functionality that are not taken care of by the client software running on users' workstations. For a fuller multilingual implementation, continue with "Providing Post Office Support for Multiple Languages" on page 1021.

Providing Post Office Support for Multiple Languages

A few aspects of GroupWise functionality are affected by the language in use by the POA running for the post office to which users belong. The POA returns certain text in the language in which it is running, not the language in use on users' workstations.

- The status information (Delivered, Opened, an so on) displayed in the Properties page of items
- The text of return notification mail receipts (if the user has enabled this type of notification)
- The sort order in the Address Book

In some circumstances, these issues can be resolved by grouping users who speak the same language into the same post office and then installing the POA in the same language that the users are using. The following sections of the *GroupWise 6.5 Administration Guide* help you with the tasks of setting up additional post offices and installing the POA for each one:

- "Creating a New Post Office" on page 147
- "Installing and Starting the POA" on page 427

At present, the POA is available in fewer languages than the GroupWise client, so this solution helps only those client users who are at least somewhat familiar with the language in use by the POA.

77 Tools for Analyzing and Correcting GroupWise Client Problems

The following tools can assist you in analyzing and correcting GroupWise® client problems.

- "GroupWise Exception Handler for the Windows Client" on page 1023
- "GroupWise Check" on page 1023

GroupWise Exception Handler for the Windows Client

In the event that the GroupWise Windows client causes an exception (or "crashes"), GroupWise generates a GroupWise Exception Report. This report contains information that is useful in analyzing the problem that the client is having so that it can be solved.

The report is saved in \temp\grpwise.rpt. The \temp directory used is the one specified by the TMP environment variable, or if not defined by TMP, the one specified by the TEMP environment variable. If neither environment variable is defined, GroupWise uses the current directory specified when grpwise.exe is started (on Windows 95/98/ME) or the windows directory (on Windows NT/2000).

Each time an exception or crash occurs, a new report is appended to grpwise.rpt. If the file reaches 100K, the oldest reports (at the beginning of the file) are deleted.

The GroupWise Exception Report contains information such as the date and time the report was generated, the exception code, fault address, date of grpwise.exe, computer and username where the exception occurred, hardware and operating system information, process modules, raw stack dumps, and call stacks.

GroupWise Check

GroupWise Check (GWCheck) is a tool that performs maintenance and repair tasks to keep GroupWise operating efficiently. It is essentially a standalone version of the Mailbox/Library Maintenance feature available in ConsoleOne®. GroupWise Check checks and repairs GroupWise user, message, library, and resource databases without having ConsoleOne and the GroupWise snap-in loaded. In addition to checking post office, user, and library databases, it also checks remote and archive databases.

- "Enabling GroupWise Check in the Windows Client" on page 1024
- "Using GroupWise Check with the Cross-Platform Client" on page 1024

Enabling GroupWise Check in the Windows Client

GroupWise Check can be installed with the GroupWise Windows client (unless you have specified in setup.cfg that it not be installed), and is available by clicking Tools > Repair Mailbox in the client in Caching and Remote modes after you complete the following:

1. Locate the directory named gwcheck. This is a subdirectory of the directory where the client is installed (usually c:\novell\groupwise).
2. Locate grpwise.exe. It is usually in c:\novell\groupwise.
3. Copy all the files in gwcheck to the directory where grpwise.exe is located.

You can now run GroupWise Check in Caching and Remote mode. The GroupWise Check dialog box is titled GroupWise Mailbox Maintenance. You can also use Ctrl+Shift when accessing a Caching or Remote mailbox to run GroupWise Check before opening the mailbox.

For detailed information about GroupWise Check, click Help or see "GroupWise Check" on page 391.

Using GroupWise Check with the Cross-Platform Client

GroupWise Check is not accessible from the Cross-Platform client but can be installed on a Linux workstation if you need to repair local databases. For installation instructions, see "Starting GWCheck on a Linux Workstation" on page 394.

NOTE: GroupWise Check is not available on Macintosh.

78 Startup Switches for the GroupWise Client

The GroupWise® client has optional startup switches that you can use when you start the program. Some of these startup switches are for your convenience, while others are necessary to run GroupWise on your particular hardware. Some switches are not available in the Cross-Platform client.

Windows Client	Cross-Platform Client
/@u-?	-@u ?
/@u-*user_ID*	-@u *user_ID*
/bl	N/A
/c	N/A
/cm	N/A
/iabs	N/A
/ipa-*IP_address_or_hostname*	-ipa *IP_address_or_hostname*
/ipp-*port_number*	-ipp *port_number*
/l-*xx*	-l *xx*
/la-network_ID	N/A
/nu	-nu
/ph-*pathname*	-ph *pathname*
/pc-*path_to_caching_mailbox*	-pc *path_to_caching_mailbox*
/pr-path_to_remote_mailbox	N/A

/@u-?

Displays a login dialog box whenever you open the GroupWise client, allowing you to supply any necessary login information.

Syntax: `/@u-?`

Example: `grpwise.exe /@u-?`

/@u-*user_ID*

Lets you use your GroupWise user ID to use the GroupWise client as yourself on another user's computer. The other user remains logged on to the network.

Syntax: `/@u-user_ID`

Example: `grpwise.exe /@u-ltanaka`

/bl

Prevents the GroupWise client logo screen from being displayed when you start the GroupWise client.

Syntax: `/bl`

Example: `grpwise.exe /bl`

This startup switch is not available in the Cross-Platform client.

/c

Checks for unopened items. If there are unopened items, the GroupWise client opens as usual. Otherwise, the GroupWise client does not start.

Syntax: `/c`

Example: `grpwise.exe /c`

This startup switch is not available in the Cross-Platform client.

/cm

Checks for unopened items. If there are unopened items, the GroupWise client opens minimized and a beep sounds. Otherwise, the GroupWise client does not start.

Syntax: `/cm`

Example: `grpwise.exe /cm`

This startup switch is not available in the Cross-Platform client.

/iabs

Initializes the Address Book when the GroupWise client starts.

Syntax: `/iabs`

Example: `grpwise.exe /iabs`

This startup switch is not available in the Cross-Platform client.

/ipa-*IP_address_or_hostname*

Lets you specify the IP address or the hostname when you are running in client/server mode.

Syntax: `/ipa-IP_address`

Example: `grpwise.exe /ipa=127.65.45.1`

/ipp-*port_number*

Lets you specify the IP port number when you are running in client/server mode.

Syntax: `/ipp-port_number`

Example: `grpwise.exe /ipp-1677`

/l-*xx*

Applies only if you have two or more language versions or language modules. This option instructs GroupWise to override the default environment language (under Environment in Options) with the language specified by the language code *xx*. The language codes are listed below. This table lists the language codes used by all Novell® products. GroupWise might not yet be available in some of the listed languages. For current information, contact your local reseller.

Language	Code
Arabic	AR
Chinese Simplified	ZH-CN
Chinese Traditional	ZH-TW
Czech	CS
Danish	DK
Dutch	NL
English	US
Finnish	SU
French	FR
German	DE
Hebrew	HE
Hungarian	MA
Italian	IT
Japanese	JA
Korean	KO
Norwegian	NO

Language	Code
Polish	PL
Portuguese	BR
Russian	RU
Spanish	ES
Swedish	SV

Syntax: `/l-xx`

Example: `grpwise.exe /l-ES`

/la-*network_ID*

Lets you use your network ID to use the GroupWise client as yourself on another user's computer. The other user remains logged on to the network.

Syntax: `/la-network_ID`

Example: `grpwise.exe /la-jgrey`

This startup switch is not available in the Cross-Platform client.

/nu

Turns off AutoRefresh. If this option is selected, click View > Refresh whenever you want to update the display to see the items currently in your mailbox.

Syntax: `/nu`

Example: `grpwise.exe /nu`

/ph-*pathname*

Lets you specify the path to the post office.

Syntax: `/ph-pathname`

Example: `grpwise.exe /ph-j:\mail\denver1`

/pc-*path_to_caching_mailbox*

Opens GroupWise in Caching mode. GroupWise must be restarted when you change from Online to Caching.

Syntax: `/pc-path_to_caching_mailbox`

Example: `grpwise.exe /pc-c:\novell\groupwise\cache`

/pr-*path_to_remote_mailbox*

Opens the GroupWise client in Remote mode. This startup switch can be used in the Target text box only.

Syntax: `/pr-path_to_remote_mailbox`

Example: `grpwise.exe /pr-c:\novell\groupwise\remote`

This startup switch is not available in the Cross-Platform client.

XV Security

79 GroupWise Passwords

Access to GroupWise® mailboxes is protected by post office security settings or GroupWise passwords. Agent passwords grant access to remote servers and to Novell® eDirectory™, and protect access to GroupWise agent status information.

- "Mailbox Passwords" on page 1033
- "Agent Passwords" on page 1036

Mailbox Passwords

When you are setting up a new GroupWise system, you need to determine what kind of password protection you want to have on users' GroupWise mailboxes before users start running GroupWise. In ConsoleOne®, you can choose where password information is obtained when users log in to GroupWise and you can set defaults under Client Options to enforce your choices. You and GroupWise client users should keep in mind that GroupWise passwords are case sensitive.

- "Using Post Office Security Instead of GroupWise Passwords" on page 1033
- "Requiring GroupWise Passwords" on page 1034
- "Managing GroupWise Passwords" on page 1034
- "Using LDAP Passwords Instead of GroupWise Passwords" on page 1036
- "Bypassing Mailbox Passwords to Respond to Corporate Mandates" on page 1036

Using Post Office Security Instead of GroupWise Passwords

When you create a new post office, you must select a security level for it.

If you select Low Security for the post office, users are not required to set passwords on their GroupWise mailboxes. However, passwordless mailboxes are completely unprotected from other users who know how to use the @u-*user_ID* startup switch.

If you select High Security for the post office, users are still not required to set passwords on their GroupWise mailboxes, but they are required to be successfully logged in to a network before they can access their own passwordless mailboxes. Users cannot access other users' passwordless mailboxes.

After you select High Security, you can further enhance post office security by requiring specific types of authentication before users can access their passwordless GroupWise mailboxes. You can require eDirectory authentication so that users must be logged into eDirectory before they can access their passwordless GroupWise mailboxes.

In spite of these passwordless solutions to GroupWise mailbox security, users are always free to set their own GroupWise passwords on their mailboxes. When they do, the post office security settings no longer apply (except for LDAP authentication as discussed below) and users will be regularly faced with both logins unless some additional password options are selected for them, as described in the following sections.

Requiring GroupWise Passwords

Users are required to set passwords on their GroupWise mailboxes if they want to access their GroupWise mailboxes in any of the following ways:

- Using Caching mode or Remote mode in the GroupWise Windows* client
- Using Caching mode in the GroupWise Cross-Platform client
- Using their Web browsers and the GroupWise WebAccess client
- Using an IMAP e-mail client
- Accessing a GroupWise mailbox as an external entity rather than as an eDirectory user

Managing GroupWise Passwords

When GroupWise passwords are in use in addition to network passwords, there are a variety of things you can do to make GroupWise password management easier for your and to make the additional GroupWise password essentially transparent for your GroupWise users.

- "Establishing a Default GroupWise Password for New Accounts" on page 1034
- "Accepting eDirectory Authentication Instead of GroupWise Passwords" on page 1034
- "Using Novell SecureLogin to Handle GroupWise Passwords" on page 1035
- "Allowing Windows to Cache GroupWise Passwords" on page 1035
- "Using Intruder Detection" on page 1035
- "Resetting GroupWise Passwords" on page 1035
- "Synchronizing GroupWise Passwords and LDAP Passwords" on page 1036

NOTE: A GroupWise password can contain as many as 64 characters and can contain any typeable characters.

Establishing a Default GroupWise Password for New Accounts

If you want to require users to have GroupWise passwords on their mailboxes, you can establish the initial passwords when you create the GroupWise accounts. In ConsoleOne, you can establish a default mailbox password to use automatically on all new GroupWise accounts, as described in "Establishing a Default Password for All New GroupWise Accounts" on page 189. Or you can set the password on each new GroupWise account as you create it.

Keep in mind that some situations require users to have passwords on their GroupWise mailboxes, as listed in "Requiring GroupWise Passwords" on page 1034.

Accepting eDirectory Authentication Instead of GroupWise Passwords

When you create users in eDirectory, you typically assign them network passwords and users must provide those passwords when they log in to the network. If you want to make GroupWise mailbox access easy for client users, you can select Allow eDirectory Authentication Instead of Password (ConsoleOne > Tools menu > GroupWise Utilities > Client Options > Password). This allows users to select No Password Required with eDirectory (GroupWise client > Tools menu > Security > Password tab).

As long as users who select this option are logged into eDirectory as part of their network login, they are not prompted by GroupWise for a password when they access their GroupWise mailboxes. If they are not logged in to eDirectory, they must provide their GroupWise passwords in order to access their GroupWise mailboxes.

Using Novell SecureLogin to Handle GroupWise Passwords

If users have Novell SecureLogin installed on their workstations, you can select Enable Single Sign-On (ConsoleOne > Tools menu > GroupWise Utilities > Client Options > Password). This allows users to select Use Single Sign-On (GroupWise client > Tools menu > Security > Password tab). Users need to provide their GroupWise mailbox password only once and thereafter SecureLogin provides it for them as long as they are logged in to eDirectory.

Allowing Windows to Cache GroupWise Passwords

If you want to allow password information to be stored on Windows workstations, you can select Allow Password Caching (ConsoleOne > Tools menu > GroupWise Utilities > Client Options > Password). This allows users to select Remember My Password (GroupWise client > Tools menu > Security > Password tab). Users need to provide their GroupWise mailbox passwords only once and thereafter Windows provides them automatically.

Using Intruder Detection

Intruder detection identifies system break-in attempts in the form of repeated unsuccessful logins. If someone cannot provide a valid username and password combination fairly quickly, then that person probably does not belong in your GroupWise system.

Intruder detection for the GroupWise Windows client is performed by the POA and is configurable. You can set the number of failed login attempts before lockout, the length of the lockout, and so on. If a user becomes locked out, you can re-enable his or her account in ConsoleOne. See "Enabling Intruder Detection" on page 465.

Intruder detection for the GroupWise WebAccess client is built in and is not configurable. After five failed login attempts, the user is locked out for 10 minutes. If a user becomes locked out, the user must wait for the lockout period to end (unless you want to restart the WebAccess Agent).

Resetting GroupWise Passwords

In ConsoleOne, you can remove a user's password from his or her mailbox in case the password has been forgotten and needs to be reset (User object > Tools menu > GroupWise Utilities > Client Options > Security > Password tab). If necessary, you can remove the passwords from all mailboxes in a post office (Post Office object > Tools menu > Mailbox/Library Maintenance > Reset Client Options).

It is easy for users to reset their own passwords in the GroupWise Windows client (Tools menu > Options > Security > Password tab). However, if this method is used when users are in Caching or Remote mode, this changes the password on their local Caching or Remote mailboxes, but does not change the passwords on their Online mailboxes. To change their Online mailbox password while in Caching or Remote mode, users must use a method they might not be familiar with (Accounts menu > Account Options > Novell GroupWise account > Properties > Advanced > Online Mailbox Password).

It is also easy for users to reset their own passwords in the GroupWise WebAccess client (Options > Password). However, you may not want users to be able to reset their GroupWise passwords from Web browsers. In ConsoleOne, you can prevent WebAccess client users from resetting their GroupWise passwords (GroupWiseWebAccess object > Application tab > Settings page). Windows client users cannot be prevented from changing their GroupWise passwords.

Synchronizing GroupWise Passwords and LDAP Passwords

There is no automatic procedure for synchronizing GroupWise passwords and eDirectory passwords. However, if you use LDAP authentication, synchronization becomes a moot point because GroupWise users are authenticated through an LDAP directory (such as eDirectory) rather than by GroupWise itself. See "Using LDAP Passwords Instead of GroupWise Passwords" on page 1036.

Using LDAP Passwords Instead of GroupWise Passwords

Instead of using GroupWise passwords, users' password information can be validated using an LDAP directory. In order for users to use their LDAP passwords to access their GroupWise mailboxes, you must define one or more LDAP servers in your GroupWise system and configure the POA for each post office to perform LDAP authentication, as described in "Providing LDAP Authentication for GroupWise Users" on page 461.

When LDAP authentication is enabled, you can control whether users can use the GroupWise client to change their LDAP passwords in ConsoleOne (Post Office object > GroupWise > Security). If you allow them to, users can change their passwords through the Security Options dialog box (GroupWise Windows client > Tools menu > Options > Security) or on the Passwords page (GroupWise WebAccess client > Options > Password). If you do not allow them to change their LDAP passwords in the GroupWise client, users will need to use a different application in order to change their LDAP passwords.

You and users can use some of the same methods to bypass LDAP passwords as you can use for bypassing GroupWise passwords. See "Accepting eDirectory Authentication Instead of GroupWise Passwords" on page 1034 and "Allowing Windows to Cache GroupWise Passwords" on page 1035.

For more information about LDAP passwords, see "Authenticating to GroupWise with Passwords Stored in an LDAP Directory" on page 1047.

Bypassing Mailbox Passwords to Respond to Corporate Mandates

Sometimes it is necessary to access user mailboxes to meet corporate mandates such as virus scanning, content filtering, or e-mail auditing that might be required during litigation. These types of mailbox access are obtain using trusted applications, third-party programs that can log into Post Office Agents (POAs) in order to access GroupWise mailboxes. For more information about using trusted application to bypass mailbox passwords, see "Trusted Applications" on page 62

Agent Passwords

Agent passwords facilitate access to remote servers where domains, post office, and document storage areas are located and access to eDirectory for synchronization of user information between GroupWise and eDirectory. They also protect GroupWise Monitor and the agent Web consoles from unauthorized access.

- "Facilitating Access to Remote Servers" on page 1037
- "Facilitating Access to eDirectory" on page 1037
- "Protecting the Agent Web Consoles" on page 1038
- "Protecting the GroupWise Monitor Web Console" on page 1038

Facilitating Access to Remote Servers

If the NetWare® POA runs on a server other than where the post office database and directory structure are located, it needs to log in to that remote server using an existing username and password. There are several ways to provide this information:

- Fill in the Remote User Name and Remote Password fields on the Post Office Settings page of the Post Office object in ConsoleOne
- Add the /dn startup switch to the POA startup file to provide the fully distinguished name of the NetWare POA object
- Add the /user and /password startup switches to the POA startup file to provide a username and password

The Windows POA also needs username and password information if it needs to access a document storage area on a server other than the one where the post office database and directory structure are located. The three methods listed above can be used for this situation as well. The Windows POA does not need username and password information in order to access the post office directory because it should already have a drive mapped to that location.

If the NetWare MTA, Internet Agent, or WebAccess Agent runs on a server other than where the domain database and directory structure are located, it needs to log in to that remote server using an existing username and password. All three of these agents support the /user and /password switches for this purpose. The MTA also supports the /dn switch parallel to the POA. You cannot currently use ConsoleOne to specify username and password information for these agents.

Providing passwords in clear text in a startup file may seem like a security risk. However, the servers where the agents run should be kept physically secure. If an unauthorized person did gain physical access, they would not be doing so for the purpose of obtaining these particular passwords. And the passwords are encrypted as they pass over the wire between servers, so the security risk is minimal.

Facilitating Access to eDirectory

If you have enabled eDirectory user synchronization, the MTA must be able to log in to eDirectory in order to obtain the updated user information.

If the eDirectory-enabled NetWare MTA is running on a different server from where the domain is located, you must add the /user and /password switches, or the /dn switch, to the MTA startup file so that the MTA can authenticate to eDirectory. The /dn switch is preferable, so that username and password information is not exposed in the MTA startup file. If the NetWare MTA is running on the same server where the domain is located, the MTA can look up the distinguished name in the domain database.

For the eDirectory-enabled Windows MTA, you must add the /user and /password switches to the MTA startup file in order to specify the network user account that the MTA should use to authenticate to eDirectory.

For more information, see "Using eDirectory User Synchronization" on page 598.

Protecting the Agent Web Consoles

When you install the POA and the MTA, they are automatically configured with an agent Web console and no password protection is provided. When you install the Internet Agent and the WebAccess Agent, you can choose whether to enable the agent Web console during installation. If you do, you can provide password protection at that time.

If you do not want agent Web console status information available to anyone who knows the agent network address and port number, you should set passwords on your agent Web console, as described in the following sections:

- "Using the POA Web Console" on page 489
- "Using the MTA Web Console" on page 617
- "Monitoring the Internet Agent through the Web Console" on page 742"Monitoring the Internet Agent through the Web Console"
- "Monitoring the WebAccess Agent through the Web Console" on page 879

If you plan to access the agent Web consoles from GroupWise Monitor, it will be most convenient if you use the same password on all agent Web consoles. That way, you can provide the agent Web console password once in GroupWise Monitor, rather than having to provide various passwords as you view the Web consoles for various agents. For information about providing the agent Web console password in GroupWise Monitor, see "Configuring Polling of Monitored Agents" on page 917.

Protecting the GroupWise Monitor Web Console

Along with the agent Web consoles, you can also provide password protection for the Monitor Web console itself, from which all the agent Web consoles can be accessed. For instructions, see "Configuring Authentication and Intruder Lockout for the Monitor Web Console" on page 924.

80 Encryption and Certificates

GroupWise® employs its own native encryption at all levels, but you can use industry-standard encryption if desired:

- "Native GroupWise Encryption" on page 1039
- "Personal Digital Certificates, Digital Signatures, and S/MIME Encryption" on page 1040
- "Server Certificates and SSL Encryption" on page 1041

Native GroupWise Encryption

GroupWise employs proprietary encryption throughout your GroupWise system:

- Messages are encrypted when sent from the GroupWise client.
- Attachments to messages are encrypted.
- The complete contents of mailboxes (Online, Caching, and Remote, along with the mailbox archive) are encrypted.
- Mailbox passwords are encrypted.
- The GroupWise Address Book and all personal address books are encrypted.
- The complete contents of GroupWise databases (domain databases, post office databases, user databases, message databases, and so on, are encrypted.
- Documents stored in libraries are encrypted.
- All information passing between workstations and servers within your GroupWise system is encrypted at all times.
- GroupWise Messenger conversations are encrypted.

Your GroupWise system is very secure without employing addition security measures. However, additional security features can be added as needed. To enhance the security of users' messages, you can install a third-party security product so that users can employ personal certificates and S/MIME encryption of messages, as described in "Personal Digital Certificates, Digital Signatures, and S/MIME Encryption" on page 1040. To enhance the security of communication between the servers in your GroupWise system, you can obtain server certificates and enable SSL encryption, as described in "Server Certificates and SSL Encryption" on page 1041.

Personal Digital Certificates, Digital Signatures, and S/MIME Encryption

If desired, you can enhance native GroupWise encryption with S/MIME encryption for GroupWise client users by installing various security providers on users' workstations, including:

- Entrust* 4.0 or higher (http://www.entrust.com)
- Microsoft* Base Cryptographic Provider 1.0 or higher (included with Internet Explorer 4.0 or higher)
- Microsoft Enhanced Cryptographic Provider 1.0 or higher (http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp)
- Microsoft Strong Cryptographic Provider (http://www.siliconprairiesc.com/spsckb/EncryptAll/strong_cryptographic_provider.htm)
- Gemplus GemSAFE Card CSP 1.0 or higher (http://www.gemplus.com)
- Schlumberger Cryptographic Provider (http://www.slb.com)

These products enable users to digitally sign and/or encrypt their messages using S/MIME encryption. When a sender digitally signs a message, the recipient is able to verify that the item was not modified en route and that it originated from the sender specified. When a sender encrypts a message, the sender ensures that the intended recipient is the only one who can read it. Digitally signed and/or encrypted messages are protected as they travel across the Internet, whereas native GroupWise encryption is removed as messages leave your GroupWise system.

Once users have installed the S/MIME security providers on their workstations, you can configure default functionality for it in ConsoleOne® (Domain, Post Office, or User object > Tools menu > GroupWise Utilities > Client Options > Send > Security tab). You can specify a URL from which you want users to obtain their S/MIME certificates. You can require the use of digital signatures and/or encryption, rather than letting users decide when to use them. You can even select the encryption algorithm and encryption key size if necessary. For more information, see "Modifying Send Options" on page 987.

After you have configured S/MIME functionality in ConsoleOne, GroupWise users must select the security provider (Tools menu > Options > Security > Send Options) and then obtain a personal digital certificate. Unless you installed Entrust, users can request certificates in the GroupWise client (Tools menu > Options > Certificates > Get Certificate). If you provided a URL, users are taken to the Certificate Authority of your choice. Otherwise, certificates for use with GroupWise can be obtained from various certificate providers, including:

- Novell, Inc. (if you have installed Novell Certificate Server 2 (http://www.novell.com/products/certserver))
- VeriSign*, Inc. (http://www.verisign.com)
- Thawte Certification (http://www.thawte.com)
- GlobalSign (http://www.globalsign.com)

NOTE: Some certificate provides charge a fee for certificates and some do not.

After users have selected the appropriate security provider and obtained a personal digital certificate, they can protect their messages with S/MIME encryption by digitally signing them (Actions > Sign Digitally) and/or encrypting them (Actions > Encrypt). Buttons are added to the GroupWise toolbar for convenient use on individual messages, or users can configure GroupWise to always use digital signatures and/or encryption (Tools menu > Options > Security > Send Options tab). The messages they send with digital signatures and/or encryption can be read by recipients using any other S/MIME-enabled e-mail products.

GroupWise client users are responsible for managing their personal digital certificates. Users can have multiple personal digital certificates. In the GroupWise client, users can view their own certificates, view the certificates they have received from their contacts, access recipient certificates from LDAP directories (see "Accessing S/MIME Certificates in an LDAP Directory" on page 1048 for details), change the trust level on certificates, import and export certificates, and so on.

The certificates are stored in the local certificate store on the user's workstation. They are not stored in GroupWise. Therefore, if a user moves to a different workstation, he or she must import the personal digital certificate into the certificate store on the new workstation, even though the same GroupWise account is being accessed.

If your system includes smart card readers on users' workstations, certificates can be retrieved from this source as well, so that after composing a message, users can sign them by inserting their smart cards into their card readers. The GroupWise client picks up the digital signature and adds it to the message.

The GroupWise client verifies the user certificate to ensure that it has not been revoked. It also verifies the Certificate Authority. If a certificate has expired, the GroupWise user receives a warning message.

For complete details about using S/MIME encryption in the GroupWise Windows client, see "Sending Secure Message (S/MIME)" in the *GroupWise 6.5 Windows Client User Guide*. S/MIME encryption is not available in the WebAccess client.

Any messages that are not digitally signed or encrypted are still protected by native GroupWise encryption as long as they are within your GroupWise system.

Server Certificates and SSL Encryption

If desired, you can enhance native GroupWise encryption with Secure Sockets Layer (SSL) communication between servers where GroupWise agents are installed. If you have not already set up SSL on your system, you must complete the following tasks:

- "Generating a Certificate Signing Request and Private Key" on page 1041
- "Submitting the Certificate Signing Request to a Certificate Authority" on page 1043
- "Creating Your Own Certificate" on page 1043
- "Installing the Certificate on the Server" on page 1044
- "Configuring the Agents to Use SSL" on page 1045

If you have already set up SSL on your system and are using it with other applications besides GroupWise, skip to "Configuring the Agents to Use SSL" on page 1045.

Generating a Certificate Signing Request and Private Key

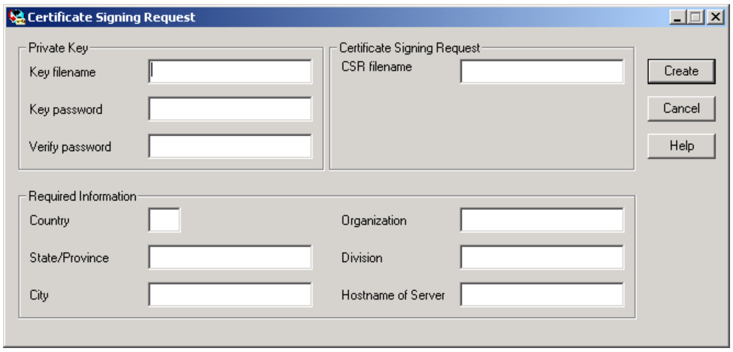
Before the GroupWise agents can use SSL, you must create a Certificate Signing Request (CSR) and obtain a public certificate file. The CSR includes the hostname of the server where the agents run. Therefore, you must create a CSR for every server where you want the GroupWise agents to use SSL. However, all GroupWise agents running on the same server can all use the same resulting certificate, so you do not need separate CSRs for different agents.The CSR also includes your choice of name and password for the private key file that must be used with each certificate. This information is needed when configuring the agents to use SSL.

One way to create a CSR is to use the GWCSRGEN utility. This utility takes the information you provide and creates a .csr file from which a public certificate file can be generated.

1 Start the GroupWise Generate CSR utility.

On Linux, the utility (gwcsrgen) is installed to the /opt/novell/groupwise/agents/bin directory. You must be logged in as root to start the utility.

On Windows, the utility (gwcsrgen.exe) is located in the \admin\utility\gwcsrgen directory either on the *GroupWise 6.5 Administrator* CD or in the GroupWise software distribution directory.



2 Fill in the fields in the Private Key box. The private key information is used to create both the Private Key file and the Certificate Signing Request file.

Key Filename: Enter a name for the Private Key file (for example, server1.key). If you don’t want the file stored in the same directory as the GWCSRGEN utility, specify a full path with the filename (for example, c:\server1.key or /opt/novell/groupwise/certs/server1.key).

Key Password: Enter the password for the private key. The password can be up to 256 characters (single-byte environments).

Verify Password: Enter the password again.

3 Fill in the fields in the Certificate Signing Request box.

CSR Filename: Enter a name for the Certificate Signing Request file (for example, server1.csr). If you don’t want the file stored in the same directory as the GWCSRGEN utility, specify a full path with the filename (for example, c:\server1.csr or /opt/novell/groupwise/certs/server1.csr).

4 Fill in the fields in the Required Information box. This information is used to create the Certificate Signing Request file. You must fill in all fields to generate a valid CSR file.

Country: Enter the two-letter abbreviation for your country (for example, US).

State/Province: Enter the name of your state or province (for example, Utah). Enter the full name. Do not abbreviate it.

City: Enter the name of your city (for example, Provo).

Organization: Enter the name of your organization (for example, Novell, Inc.).

Division: Enter your organization’s division that this certificate is being issued to (for example, Novell Product Development).

Hostname of Server: Enter the DNS hostname of the server where the server certificate will be used (for example, dev.provo.novell.com).

5. Click Create to generate the CSR file and Private Key file.

   The CSR and Private Key files are created with the names and in the locations you specified in the Key Filename and CSR Filename fields.

Submitting the Certificate Signing Request to a Certificate Authority

To obtain a server certificate, you can submit the Certificate Signing Request (*server_name*.csr file) to a Certificate Authority. If you have not previously used a Certificate Authority, you can use the keywords "Certificate Authority" to search the Web for Certificate Authority companies. The Certificate Authority must be able to provide the certificate in Base64/PEM or PFX format.

The process of submitting the CSR varies from company to company. Most provide online submission of the request. Please follow their instructions for submitting the request.

Creating Your Own Certificate

The Novell® Certificate Server™, which runs on a NetWare® server with Novell eDirectory™, enables you to establish your own Certificate Authority and issue server certificates for yourself. For complete information, see the Novell Certificate Server Web site (http://www.novell.com/products/certserver).

To quickly create your own public certificate in ConsoleOne:

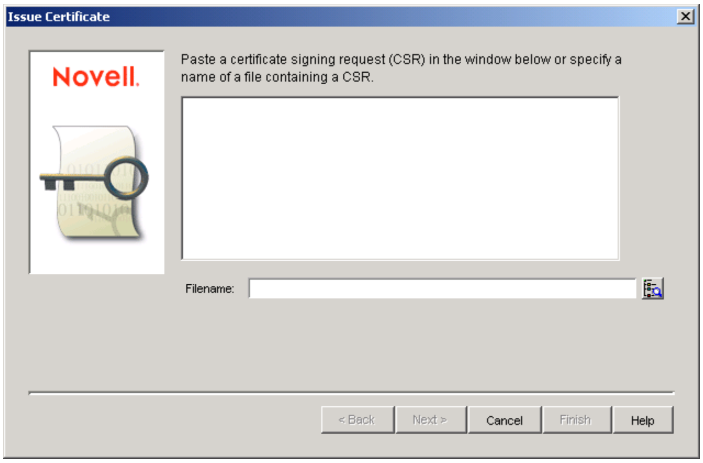
1. Click Help > About Snap-ins to see if the Certificate Server snap-in to ConsoleOne is installed.

   If it is not installed, you can obtain it from Novell Product Downloads (http://download.novell.com/pages/PublicSearch.jsp). If you are using eDirectory on Linux, the Certificate Server snap-in is installed by default.

   NOTE: You can create a server certificate in Novell iManager, as well as in ConsoleOne, using steps similar to those provided below.

2. Browse to and select the container where your Server object is located.

3. Click Tools > Issue Certificate.


Issue Certificate

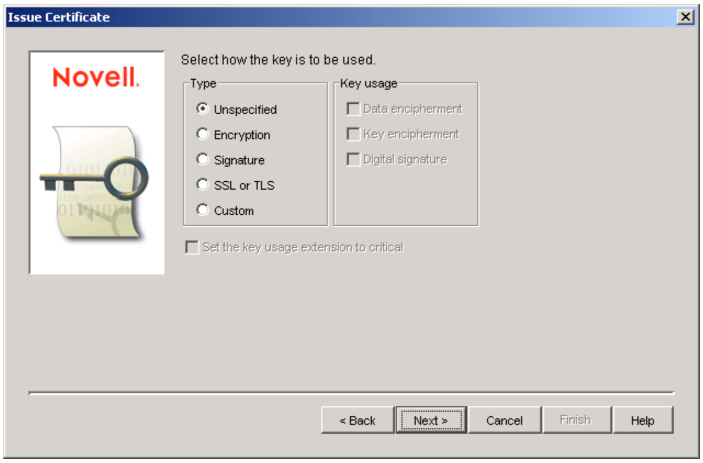
Paste a certificate signing request (CSR) in the window below or specify a name of a file containing a CSR.

Filename:

4. Browse to and select the CSR file created by GWCSRGEN in "Generating a Certificate Signing Request and Private Key" on page 1041, then click Next.

   By default, your own organizational certificate authority signs the request.

5 Click Next.



Issue Certificate

Select how the key is to be used.

Type

● Unspecified

○ Encryption

○ Signature

○ SSL or TLS

○ Custom

Key usage

□ Data encipherment

□ Key encipherment

□ Digital signature

□ Set the key usage extension to critical

6 In the Type box, select Custom.

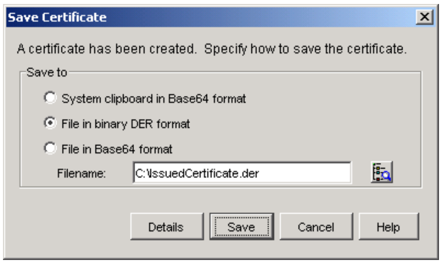
7 In the Key Usage box, select all three usage options.

8 Click Next.

9 In the Validity Period field, select the length of time you want the certificate to be valid.

You might want to change the setting to a longer period of time to best meet the needs of your organization.

10 Click Next, view the summary information, then click Finish.



Save Certificate

A certificate has been created. Specify how to save the certificate.

Save to

○ System clipboard in Base64 format

● File in binary DER format

○ File in Base64 format

Filename: C:\IssuedCertificate.der

11 Select File in Base64 Format.

12 Specify the path and filename for the certificate.

Limit the filename to 8 characters. Retain the .b64 extension.

13 Click Save.

Installing the Certificate on the Server

After processing your CSRs, the Certificate Authority returns to you a public certificate (*server_name*.crt) file and a private key (*server_name*.key) file for each CSR. The certificate file might have a different suffix, such as .pem or .pfx. The suffix is unimportant as long as the file format is correct.

If you used the Issue Certificate feature in ConsoleOne, the public certificate file has the .b64 extension and you use the private key file generated by GWCSRGEN in "Generating a Certificate Signing Request and Private Key" on page 1041.

Copy the files to any convenient location on each server. The location must be accessible to the GroupWise agents that run on the server.

Configuring the Agents to Use SSL

To configure the agents to use SSL you must first enable them for SSL and then provide certificate and key file information. For detailed instructions, see the following sections:

- “Enhancing Post Office Security with SSL Connections to the POA” on page 458
- “Enhancing Domain Security with SSL Connections to the MTA” on page 589
- Securing Internet Agent Connections Via SSL in “Internet Agent” on page 659
- Securing WebAccess Agent Connections Via SSL in “WebAccess” on page 803

81 LDAP Directories

LDAP (Lightweight Directory Access Protocol) is a standard Internet protocol for accessing commonly used network directories. If you are new to GroupWise® or LDAP, you might find it useful to review TID 2955731: GroupWise and LDAP (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2955731.htm), which provides an overview of LDAP and explains the two address-book-related ways that GroupWise makes use of LDAP. This section briefly summarizes the address book usages of LDAP and explains how LDAP can also be used to store security information such as passwords and certificates for use with GroupWise.

- "Accessing Public LDAP Directories from GroupWise" on page 1047
- "Offering the GroupWise Address Book as an LDAP Directory" on page 1047
- "Authenticating to GroupWise with Passwords Stored in an LDAP Directory" on page 1047
- "Accessing S/MIME Certificates in an LDAP Directory" on page 1048

Accessing Public LDAP Directories from GroupWise

The GroupWise client uses LDAP to provide access to directory services such as Bigfoot* and Switchboard*. This enables GroupWise users to select e-mail addresses from these popular directory services and add them to their personal GroupWise address books. See "Using LDAP in the Address Book" in "Using the Address Book" in the *GroupWise 6.5 Windows Client User Guide*.

Offering the GroupWise Address Book as an LDAP Directory

The GroupWise Internet Agent uses LDAP to make the GroupWise address book available to any LDAP-enabled client. This enables users of other e-mail clients to define GroupWise address books as LDAP directories from which they can select e-mail addresses. See"Configuring LDAP Services" in "Internet Agent" in the *GroupWise 6.5 Administration Guide*. See also Chapter 83, "Address Book Security," on page 1051.

Authenticating to GroupWise with Passwords Stored in an LDAP Directory

Enabling LDAP authentication for the POA is independent of these LDAP address book features. You need to enable LDAP authentication when you want the POA to authenticate the user's password in an LDAP directory rather than looking for a password in the user's GroupWise account information. The POA can make use of the following LDAP capabilities:

- "Access Method" on page 1048
- "LDAP Username" on page 1048

When you understand these LDAP capabilities, you are ready to set up LDAP authentication for your GroupWise users. See "Providing LDAP Authentication for GroupWise Users" on page 461.

Access Method

On a server-by-server basis (ConsoleOne > GroupWise System Operations > LDAP Servers), you can specify whether you want each LDAP server to respond to authentication requests using a bind or a compare.

- **Bind:** With a bind, the POA essentially logs in to the LDAP server. When responding to a bind request, most LDAP servers enforce password policies such as grace logins and intruder lockout, if such policies have been implemented by the LDAP directory.
- **Compare:** With a compare, the POA provides the user password to the LDAP server. When responding to a compare request, the LDAP server compares the password provided by the POA with the user's password in the LDAP directory, and returns the results of the comparison. Using a compare connection can provide faster access because there is typically less overhead involved because password policies are not being enforced.

Regardless of whether the POA is submitting bind requests or compare requests to authenticate GroupWise users, the POA can stay connected to the LDAP server as long as authentication requests continue to occur before the connection times out. This provides quick response as users are accessing their mailboxes.

LDAP Username

On a post office-by-post office basis (ConsoleOne > Post Office object > GroupWise tab > Security page), you can decide what username you want the POA to use when accessing the LDAP server.

- **LDAP Username Login:** If you want the POA to access the LDAP server with specific rights to the LDAP directory, you can provide a username for the POA to use when logging in. The rights of the user determine what information in the LDAP directory will be available during the authentication process.
- **Public or Anonymous Login:** If you do not provide a specific LDAP username as part of the post office LDAP configuration information, then the POA accesses the LDAP directory with a public or anonymous connection. Only public information is available when using such a login.

Accessing S/MIME Certificates in an LDAP Directory

Just as the POA can access user password information in an LDAP directory, the GroupWise client can access recipients' digital certificates in an LDAP directory. See "Searching for Recipient Encryption Certificates Using LDAP" in "Sending Secure Message (S/MIME)" in the GroupWise 6.5 Windows Client User Guide.

When a certificate is stored on an LDAP server, the GroupWise client searches the LDAP server every time the certificate is used. Certificates from LDAP servers are not downloaded into the local certificate store on the user's workstation. To facilitate this process, the user must select a default LDAP directory in the LDAP address book (LDAP Address Book > Directories > Set as Default) and enable searching (Tools > Options Security > Send > Advanced Options > Search for Recipient Encryption Certificates in the Default LDAP Directory). An advantage to this is that recipients' certificates are available no matter what workstation the GroupWise user sends the message from.

82 Message Security

The GroupWise® client accommodates users' preferences for security and privacy when sending messages. Users can:

- Sign a message with standardized text (Tools menu > Options > Environment > Signature).
- Sign a message with an Electronic Business Card (vCard) (Tools menu > Options > Environment > Signature).
- Digitally sign and/or encrypt a message. See "Personal Digital Certificates, Digital Signatures, and S/MIME Encryption" on page 1040.
- Give a message a security classification (Mail To > Send Options > General > Classification > Proprietary, Confidential, Secret, Top Secret, or For Your Eyes Only).
- Conceal the subject of an e-mail message (Mail To > Send Options > Security > Conceal Subject).
- Mark messages and appointments private so that proxy users cannot see them. (Actions > Mark Private).
- Attach a password-protected document to a message and have the recipient prompted to supply the password before the recipient can open the document.
- Require a password in order to mark a Routing Slip completed (Tools menu > Options > Send >Security tab > Require Password to Complete Routed Item). This can prevent a user who is proxied to the mailbox from marking the item completed, or if multiple users proxy to the mailbox, it can be used to ensure that only the user for whom the item was intended can complete it.

In addition, if the users in your GroupWise system exchange messages with users in other GroupWise systems, you can set preferences to control what types of information pass between the two systems. For example, you can prevent external GroupWise users from performing busy searches or obtaining message delivery status. See "System Preferences" on page 44.

83 Address Book Security

One of the purposes of the Address Book is to make user information available to all GroupWise® users. However, there might be types of information that you do not want to display.

- "eDirectory Information Displayed in the Address Book" on page 1051
- "Controlling GroupWise Object Visibility in the Address Book" on page 1051
- "Suppressing the Contents of the User Description Field" on page 1051

eDirectory Information Displayed in the Address Book

The Address Book displays information stored in Novell® eDirectory™ for users, resources, and distribution lists in your GroupWise system. By default, the following information is displayed:

- Name
- Office phone number
- Department
- Fax number
- User ID

You can configure the Address Book to display more or less information to meet the needs of your users. See "Determining Fields, Field Order, and Sort Order for the Address Book" on page 81.

By default, all users, resources, and distribution lists that you create in eDirectory are displayed in the Address Book and are available to all GroupWise users.

Suppressing the Contents of the User Description Field

By default, when you display details about a user in the Address Book, the information in the Description field of the User object in eDirectory is displayed. If you keep confidential information in the Description field of the User object, you can prevent this information from appearing the GroupWise Address Book. See "Preventing the User Description Field from Displaying in the Address Book".

Controlling GroupWise Object Visibility in the Address Book

You might need to create users, resources, or distribution lists that are not available to all GroupWise users. You can accomplish this by restricting the set of users that can see such objects in the Address Book. You can make such objects visible only to the members of a domain, only to the members of a post office, or to no one at all. An object does not need to be visible to be addressable. For instructions, see "Controlling Object Visibility in the Address Book" on page 86.

Controlling GroupWise Object Visibility between GroupWise Systems

If you synchronize your GroupWise system with other GroupWise systems to simplify addressing for users of both systems, you can control what information from your Address Book you want to be available in the Address Books of other GroupWise systems. For instructions, see "Exchanging Information Between Systems" in "Connecting to GroupWise 5.x and 6.x Systems" in the *GroupWise 6.5 Multi-System Administration Guide*.

84 GroupWise Administrator Rights

To administer GroupWise®, a user needs the appropriate file system rights and Novell® eDirectory™ rights. The following sections provide information to help you configure GroupWise administrator rights to meet the needs of your environment:

- "Setting Up a GroupWise Administrator as an Admin Equivalent" on page 1053. If security is not an issue, you can set up your GroupWise administrators as Admin equivalents. This gives them full eDirectory rights to administer GroupWise. It will also give them full file system rights to NetWare® servers.
- "Assigning Rights Based on Administration Responsibilities" on page 1053. If security is an issue, you can restrict GroupWise administrators' file system and eDirectory rights to only those required to administer GroupWise.
- "eDirectory Object and Properties Rights" on page 1061. This section lists all eDirectory objects and properties associated with GroupWise.
- "Granting or Removing Object and Property Rights" on page 1064. This section explains how to grant or remove a user's rights to eDirectory objects and their properties.

Setting Up a GroupWise Administrator as an Admin Equivalent

The easiest way to ensure that a GroupWise administrator has all necessary eDirectory rights and NetWare file system rights is to make the administrator an Admin equivalent. Unless you have implemented multiple administrators who have different roles and access rights (for example, a server administrator, a printer administrator, and a GroupWise administrator), we suggest you make your GroupWise administrator an Admin equivalent.

1. In ConsoleOne®, right-click the GroupWise administrator's User object, then click Properties.
2. Click the Memberships tab, then click Security Equal To to display the Security Equal To page.
3. Click Add to display the Select Objects dialog box.
4. Browse for and select the Admin object, then click OK.

   The Admin object should now be displayed in the Security Equal To list.
5. Click OK.

Assigning Rights Based on Administration Responsibilities

Making a GroupWise administrator an Admin equivalent gives the GroupWise administrator all eDirectory rights required to administer GroupWise. It will also give him or her full file system rights to NetWare servers. To increase security or to support a distributed administration model, you can assign rights to your GroupWise administrators based on their administration responsibilities. For example,

- If you have only one GroupWise administrator (a centralized GroupWise administration model), you can give the administrator rights only to the eDirectory objects and file systems that are used for GroupWise.
- If you have multiple administrators who are each responsible for a domain (a distributed GroupWise administration model), you can restrict their rights to only those eDirectory objects and file systems associated with their GroupWise domain.
- If you have one administrator whom you want to control all links between domains, you can assign rights to the eDirectory objects and file systems associated with domains links.

The following two sections, "File System Rights" on page 1054 and "eDirectory Rights" on page 1054, provide general information about the file system rights and eDirectory object and property rights needed to perform GroupWise administration tasks.

The final section, "Common Types of GroupWise Administrators" on page 1058, lists some common types of GroupWise administrators (for example, Domain administrator and Post Office administrator) and the specific file system and eDirectory rights they need.

File System Rights

A GroupWise administrator must have an account (or security equivalence) that provides the following rights to the directories listed below:

Directory	NetWare Rights	Windows Permissions
sys:\public (for ConsoleOne and GroupWise Administrator snap-ins)	Read File Scan	Not applicable
Any GroupWise system directory the administrator is responsible for. This includes: ◆ domain directories ◆ post office directories ◆ software distribution directories ◆ library storage area directories	Read Write Create Erase Modify File Scan Access Control	Full Control
Any directory in which the GroupWise agents are installed. For NetWare, the default directory is sys:\system. For Windows NT*/2000, the default directory is c:\grpwise (for the MTA, POA, and Internet Agent) and c:\webacc (for the WebAccess Agent).	Read Write Create Erase Modify File Scan Access Control	Full Control

eDirectory Rights

The eDirectory object and property rights an administrator requires depend on the administrative tasks he or she needs to perform. In GroupWise administration, there are five basic tasks an administrator can perform:

- Create and delete objects (for example, domains, post offices, gateways, agents, libraries, resources, external entities, and distribution lists).

- Modify object properties (for example, moving a GroupWise user from one post office to another or deleting a GroupWise user from a distribution list).
- Modify link information (for example, defining whether Domain 1 links directly to Domain 3 or indirectly to Domain 3 through Domain 2).
- Perform system operations (for example, managing software distribution directories, creating administrator-defined fields, and setting up eDirectory user synchronization).
- Perform maintenance operations (for example, rebuilding domain and post office databases, analyzing and fixing user and message databases, and changing a user's client options).

Creating and Deleting Objects

The following rules apply to creating or deleting a GroupWise object (for example, domain, post office, gateway, agent, library, resource, external entity, or distribution list):

- To create a GroupWise object, the administrator must have Create object rights in the container where he or she is creating the object. To delete a GroupWise object, the administrator must have Delete object rights to the GroupWise object's container.
- If creating or deleting the object requires modification of a second object's properties, the administrator must have Read and Write rights to the second object's NGW: GroupWise ID property and all other affected properties. For example, when you create a distribution list, the list is assigned to a post office. Therefore, the administrator needs Read and Write rights to the post office object's NGW: GroupWise ID property and NGW: Distribution List Member property.

For information about giving a user rights to an object or an objects's properties or restricting a user's rights to an object or an object's properties, see "Granting or Removing Object and Property Rights" on page 1064.

Modifying Object Properties

Each eDirectory object has certain properties that hold information about the object. For example, a User object includes Full Name, Given Name, Last Name, Network Address, and Title properties. The following rules apply to modifying an object's properties:

- Each object has an NGW: GroupWise ID property. The administrator must always have Read and Write rights to the NGW: GroupWise ID property for the object being modified. Without rights to the NGW: GroupWise ID property, no modifications can be made to any of the object's GroupWise properties.
- The administrator must have Read and Write rights to the property being modified. For example, to change a user's visibility within the GroupWise system, the administrator requires Read and Write rights to the user object's NGW: GroupWise ID property and NGW: Visibility property.
- If the modification affects a second object's properties, the administrator must have Read and Write rights to the second object's affected properties. For example, when you move a user from one post office to another, the move affects properties for 1) the User object, 2) the Post Office object from which you are moving the user (the source post office) and 3) the Post Office object to which you are moving the user (the target post office). Therefore, the administrator must have 1) Read and Write rights for the User object's NGW: GroupWise ID property and NGW: Post Office property, 2) Read and Write rights for the source post office object's NGW: GroupWise ID property and Members property, and 3) Read and Write rights for the target post office object's NGW: GroupWise ID property and Members property.

Modifications to an object can fail for the following reasons:

- The administrator does not have the appropriate rights to the object’s properties. For example, to restrict an administrator from moving a user from one post office to another, you could 1) not give the administrator Read and Write rights to the source or target post office object’s NGW: Members property or 2) not give the administrator Read and Write rights to the user object’s NGW: Post Office property.
- The administrator, in addition to modifying properties he or she has rights to, attempts to modify a property he or she does not have rights to modify. For example, if an administrator has rights to modify a user’s mailbox ID and visibility but does not have rights to modify the mailbox expiration date, any modifications made to the mailbox ID and visibility will fail if the administrator tries to modify the mailbox expiration date at the same time.

In general, a GroupWise administrator should have Read and Write rights to all GroupWise properties for the objects he or she needs to administer. This ensures that the administrator will be able to modify all GroupWise information for the objects. In addition, an administrator should also have Read and Write rights to other eDirectory properties used by GroupWise. For example, Full Name is an eDirectory User object property used by GroupWise. For a list of GroupWise objects, GroupWise object properties, associated eDirectory object properties, see “eDirectory Object and Properties Rights” on page 1061.

For information about giving a user rights to modify an object’s properties or restricting a user’s rights to modify an object’s properties, see “Granting or Removing Object and Property Rights” on page 1064.

Modifying Link Information

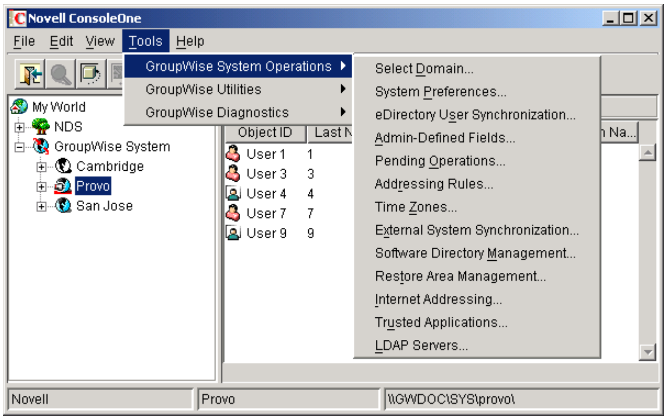
By default, when an administrator creates a domain or post office, the links to other domains or post offices are automatically created. Because there are many different ways you can configure your domain and post office links, you can use the Link Configuration utility to modify how domains and post offices are linked together. You can also use object and property rights to determine which administrators have the ability to modify link information. The following rules apply to modifying link information:

- To modify the links for post offices within a domain, the administrator must have Read and Write rights to the NGW: GroupWise ID property for the Domain object and the Post Office objects. In addition, the administrator must have Write rights to the NGW: Link Configuration property for the Domain object.
- To modify the links between domains, the administrator must have Read and Write rights to the NGW: GroupWise ID property for each Domain object, and Write rights to the NGW: Link Configuration property for each Domain object.

Because correct domain and post office links are essential to the proper functioning of your GroupWise system, you might want to assign link configuration tasks to a single administrator and restrict other administrators’ abilities to modify link information. Or, if you have a multiple-domain system with multiple administrators, you could have one administrator responsible for all domain links and the other administrators responsible for the post office links for their domains. For information about giving a user rights to an object’s properties (or restricting a user’s rights to an object’s properties), see “Granting or Removing Object and Property Rights” on page 1064.

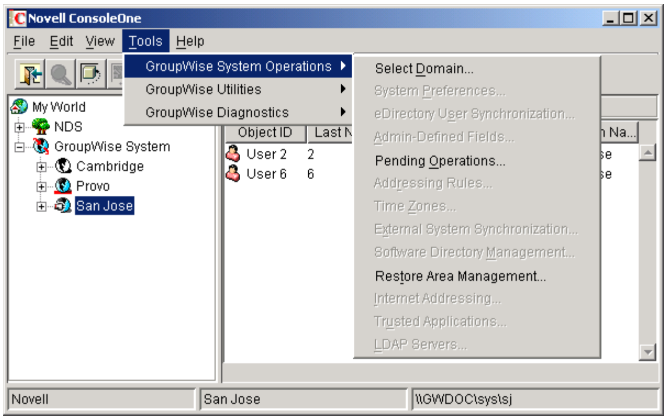
Performing System Operations

The system operations that a GroupWise administrator can perform in ConsoleOne are listed on the Tools > GroupWise System Operations menu.



The Select Domain, Pending Operations, and Restore Area Management operations are always available to GroupWise administrators. To perform any of the other system operations, an administrator must have Read and Write rights to the NGW: GroupWise ID property for the primary Domain object. In GroupWise systems that span multiple eDirectory trees, the administrator's current tree must be the tree in which the primary Domain object is located.

You can restrict the ability to perform system operations (other than Select Domain, Pending Operations, and Restore Area Management) to only those GroupWise administrators who connect to the primary domain database. To do so, you use the Restrict System Operations to Primary Domain option (Tools menu > GroupWise System Operations > System Preferences > Admin Lockout). Administrators connected to secondary domain databases would see the GroupWise System Operations menu with only the Select Domain, Pending Operations, and Restore Area Management options available.



For information about giving a user rights to an object's properties or restricting a user's rights to an object's properties, see "Granting or Removing Object and Property Rights" on page 1064.

Performing Maintenance Operations

To perform maintenance operations such as validating, recovering, or rebuilding domain databases; fixing user, resource, or post office databases; or changing a user's client options, an administrator must have Read and Write rights to the NGW: GroupWise ID property for the object being modified. For example, to rebuild a domain database, an administrator requires Read and Write rights to the NGW: GroupWise ID property for the Domain object. Or, to change a user's client options, an administrator requires Read and Write rights to the NGW: GroupWise ID property for the User object.

For information about giving a user rights to an object's properties or restricting a user's rights to an object's properties, see "Granting or Removing Object and Property Rights" on page 1064.

Common Types of GroupWise Administrators

The following sections provide information about assigning directory, object, and property rights to some common types of GroupWise administrators:

- "Domain Administrator" on page 1058
- "Post Office Administrator" on page 1059
- "Link Configuration Administrator" on page 1060

Domain Administrator

A Domain administrator is a GroupWise administrator who has all file system and eDirectory rights needed to create and maintain a single GroupWise domain.

File System Rights

A Domain administrator requires the file system rights listed in the following table.

Directory	NetWare Rights	Windows Permissions
sys:\public (for ConsoleOne and GroupWise Administrator snap-ins)	Read File Scan	Not applicable
Any GroupWise system directory the administrator is responsible for. This includes: ◆ domain directories ◆ post office directories ◆ software distribution directories ◆ library storage area directories If the domain is not yet created, it will be necessary to give the administrator rights to the directories where it will be created.	Read Write Create Erase Modify File Scan Access Control	Full Control
The GroupWise agent directories. For NetWare, the default directory is sys:\system. For Windows, the default directory is c:\grpwise.	Read Write Create Erase Modify File Scan Access Control	Full Control

eDirectory Rights

A Domain administrator requires Read and Write rights to properties for the objects listed below.

- **Domain object:** Only the domain the administrator is responsible for unless he or she will also configure domain links. If so, the administrator also needs rights to the NGW: GroupWise ID and NGW: Link Configuration properties for the other Domain objects.
- **Post Office objects:** All post offices in the domain.
- **Gateway objects:** All gateways in the domain.
- **User objects:** All users in the domain.
- **Resource objects:** All resources in the domain.
- **Distribution List objects:** All distribution lists in the domain.
- **Library objects:** All libraries in the domain.
- **Agent objects:** All MTAs and POAs in the domain.
- **External Entity objects:** All resources in the domain.

In most cases, the administrator does not need rights to all of the object properties. After reviewing the list of objects, if you want to restrict an administrator's rights to only the required properties, see "eDirectory Object and Properties Rights" on page 1061.

In addition, the administrator must have Create and Delete rights in any container in which one of the objects listed above will be created or deleted.

For a listing of the explicit object properties to which the administrator requires rights, see "eDirectory Object and Properties Rights" on page 1061.

Post Office Administrator

A Post Office administrator is a GroupWise administrator who has all file system and eDirectory rights needed to create and maintain a single GroupWise post office.

File System Rights

A Post Office administrator requires the file system rights listed in the following table.

Directory	NetWare Rights	Windows Permissions
sys:\public (for ConsoleOne and GroupWise Administrator snap-ins)	Read File Scan	Not applicable
The domain directory	Read Write Create Erase Modify File Scan Access Control	Full Control

Directory	NetWare Rights	Windows Permissions
The following directories: ◆ post office directory ◆ library storage area directories for libraries assigned to the post office	Read Write Create Erase Modify File Scan Access Control	Full Control
The directory for the Post Office Agent. For NetWare, the default directory is sys:\system. For Windows, the default directory is c:\grpwise.	Read Write Create Erase Modify File Scan Access Control	Full Control

eDirectory Rights

A Post Office administrator requires Read and Write rights to properties for the objects listed below.

In most cases, the administrator does not need rights to all of the object properties. After reviewing the list of objects, if you want to restrict an administrator's rights to only the required properties, see "eDirectory Object and Properties Rights" on page 1061.

- **Post Office object:** Only the post office that the administrator is responsible for.
- **User objects:** All users with accounts on the post office.
- **Resource objects:** All resources assigned to the post office.
- **Distribution List objects:** All distribution lists assigned to the post office.
- **Library objects:** All libraries assigned to the post office.
- **Agent objects:** Only the post office's POA.
- **External Entity objects:** All external entities with accounts on the post office.

In addition, the administrator must have Create and Delete rights in any container in which one of the objects listed above will be created or deleted.

Link Configuration Administrator

A Link Configuration administrator has all file system and eDirectory rights needed to create and maintain the links between GroupWise domains.

File System Rights

A Link Configuration administrator requires the file system rights listed in the following table.

Directory	NetWare Rights	Windows Permissions
sys:\public (for ConsoleOne and GroupWise Administrator snap-ins)	Read File Scan	Not applicable

Directory	NetWare Rights	Windows Permissions
Domain directory	Read Write Create Erase Modify File Scan	Full Control

eDirectory Rights

A Post Office administrator requires Read and Write rights to the properties for the objects listed below.

Object	Property
Domain (all domains)	NGW: GroupWise ID NGW: Link Configuration

eDirectory Object and Properties Rights

The table below lists the GroupWise objects and their properties.

Some properties are specific only to GroupWise. GroupWise-specific properties begin with NGW or ngw. Other properties are common eDirectory properties used by GroupWise objects. Common eDirectory properties do not begin with NGW or ngw.

Object	Property
Domain	NGW: File ID NGW: GroupWise ID NGW: Language NGW: Link Configuration NGW: Location NGW: Network Type NGW: Time Zone ID NGW: Type NGW: Version ngwDefaultWebAccess CN Description Member

Object	Property
Post Office	NDA: Port NGW: Access Mode NGW: Distribution List Member NGW: Domain NGW: File ID NGW: GroupWise ID NGW: Language NGW: Library Member NGW: Location NGW: Network Type NGW: Resource Member NGW: Time Zone ID NGW: Version ngwDefaultWebAccess ngwLDAPServerAddress CN Description Member
Gateway	NGW: Domain NGW: File ID NGW: GroupWise ID NGW: Language NGW: Location NGW: Platform NGW: Time Zone ID NGW: Type ngwProviderComm ndaReferenceList ndaServiceList ndaXISSettings CN Description
User	NGW: Account NGW: File ID NGW: Gateway Access NGW: GroupWise ID NGW: Mailbox Expiration Date NGW: Object ID NGW: Post Office NGW: Visibility ngwNLSInfo Department Description EMail Address Fax Number Given Name Internet EMail Address Last Name Telephone Title

Object	Property
Resource	NGW: File ID NGW: GroupWise ID NGW: Owner NGW: Post Office NGW: Type NGW: Visibility CN Description
Distribution List	NGW: Blind Copy Member NGW: Carbon Copy Member NGW: GroupWise ID NGW: Post Office NGW: Visibility CN Description Member
Library	NGW: Archive Max Size NGW: Document Area Size NGW: File ID NGW: GroupWise ID NGW: Library Display Name NGW: Post Office NGW: Starting Version Number CN Description Member
Agent	NGW: File ID NGW: GroupWise ID NGW: Platform NGW: Type ngwProxyServerAddress ndaServiceList ndaXISSettings CN Description Network Address
External Entity	NGW: Account ID NGW: External Net ID NGW: File ID NGW: GroupWise ID NGW: Mailbox Expiration Time NGW: Object ID NGW: Post Office NGW: Visibility Department Description EMail Address Fax Number Given Name Internet EMail Address Last Name Telephone Title

Granting or Removing Object and Property Rights

You can use trustee assignments to grant or restrict rights to an object and its properties. The following steps provide one way to grant or remove a user's rights to an object or its properties. For additional methods, see your eDirectory documentation.

1. Right-click the object in the eDirectory tree, then click Trustees of this Object.
2. Click Add Trustee to display the Select Object dialog box.
3. Browse for and select the User object, then click OK to display the Rights Assigned to Selected Objects dialog box.
4. Set the object and property rights you want. If necessary, add additional properties. Click Help for additional information.
5. Click OK when finished.

85 GroupWise Agent Rights

When you create domains and post offices, ConsoleOne® creates the directory structures and Agent objects with all the required rights to enable the agents to function properly, regardless of link type between locations and including requirements for Novell® eDirectory™ user synchronization. No manual adjustment of agent rights is necessary in GroupWise 6.*x*.

You can check the POA's rights to the post office directory by starting it using the /rights switch in the POA startup file.

86 GroupWise User Rights

GroupWise® users require specific Novell® eDirectory™ rights and, in some cases, specific file system rights in order for the GroupWise client to function properly. The following sections provide information about the required rights and how to supply them.

- "eDirectory Rights" on page 1067
- "File System Rights" on page 1069

eDirectory Rights

By default, ConsoleOne® is configured to automatically provide a GroupWise user's required eDirectory rights when you add the user to a post office. You can, however, configure GroupWise Administrator to not assign rights automatically, in which case you would need to manually assign eDirectory rights.

The following sections provide information about how to configure ConsoleOne to automatically set GroupWise users' eDirectory rights and how to manually set these rights:

- "Configuring ConsoleOne to Automatically Set eDirectory Rights When Creating User Accounts" on page 1067
- "Manually Granting eDirectory Rights" on page 1068

Configuring ConsoleOne to Automatically Set eDirectory Rights When Creating User Accounts

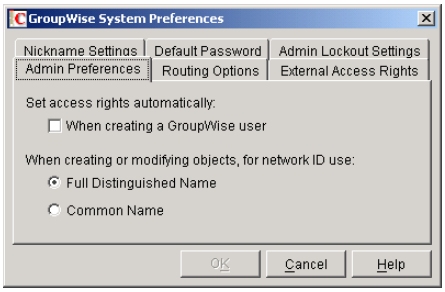
By default, the GroupWise Administrator snap-in for ConsoleOne is configured to automatically set the eDirectory rights required by a GroupWise user. This is done when you create the user's GroupWise account.

For GroupWise Administrator to be able to set these rights, you must have sufficient administrative rights to eDirectory. If you don't have sufficient rights to manually set the user's access rights, GroupWise Administrator will not have sufficient rights to set them automatically. In general, we recommend that you be an Admin equivalent. For more information, see Chapter 84, "GroupWise Administrator Rights," on page 1053.

If you choose not to grant eDirectory rights automatically, you will want to manually set the rights to ensure that users have appropriate access. For instructions, see "Manually Granting eDirectory Rights" on page 1068.

To configure whether or not GroupWise Administrator automatically assigns rights to users when you create GroupWise accounts:

1. In ConsoleOne, click the Tools menu > GroupWise System Operations > System Preferences to display the GroupWise System Preferences dialog box.



Set access rights automatically:

□ When creating a GroupWise user

When creating or modifying objects, for network ID use:

● Full Distinguished Name

○ Common Name

2. To have GroupWise Administrator automatically set access rights, select the Set Access Rights Automatically When Creating a GroupWise User option.

   or

   To turn off this option, deselect the Set Access Rights Automatically When Creating a GroupWise User option.

3. Click OK to save your changes.

Manually Granting eDirectory Rights

At startup, the GroupWise client must know the following:

- The post office where the user has an account.
- Whether to connect to the user's post office in direct access mode or client/server access mode.

The user can supply this information in the GroupWise Startup dialog box that appears or use the /ph-*path_to_post_office*, /ipa-*IP_address*, /ipp-*TCP_port*, and /@u-*userID* startup options.

If you do not want users to have to supply this information, you can give users rights to the eDirectory objects shown below. When a user has rights to the objects, the GroupWise client can read the object's information in eDirectory to determine the user's post office and access mode. This requires users to be logged in to eDirectory.

Object and Properties	Rights
User object	Browse
NGW:Post Office	Read
Post Office object	Browse
NGW:Location	Read
NGW:Access Mode	Read
POA object	Browse
NGW:Type	Read
Network Address	Read

GroupWise Name Server (NGWNAMESERVER)

The following information applies to users running the GroupWise client in client/server access mode.

If you do not want to provide eDirectory rights to GroupWise users as explained above, or if you have GroupWise users who don't log in to eDirectory, you can set up a GroupWise name server.

A GroupWise name server enables users to access their post office without knowing the IP address and port number of the POA.

The GroupWise name server is a DNS host entry for one of the POAs in your GroupWise system. At startup, the GroupWise client automatically looks for the GroupWise name server. When a user reaches the POA designated as the GroupWise name server, the POA redirects the user to the IP address and port number of the POA that services the user's post office.

The primary GroupWise name server must be named ngwnameserver. You can set up one backup GroupWise name server and name it ngwnameserver2. Both POAs must use the default TCP port of 1677.

To set up a GroupWise name server:

1. Use your tool of choice for modifying DNS.
2. Create an entry for the IP address of the POA you want to designate as the primary GroupWise name server, then give it the hostname ngwnameserver.
3. Create an entry for the IP address of the POA you want to designate as the backup GroupWise name server, then give it the hostname ngwnameserver2.

File System Rights

Listed below are the locations you need to consider when assigning file system rights to GroupWise users:

- **Domain Directory:** Users do not require file system access to the domain directory.
- **Post Office Directory:** The recommended post office access mode for the GroupWise client is client/server (TCP/IP), which means that the user does not require file system access to the post office. Therefore, ConsoleOne does not assign any file system rights when you add a user to a post office.

  If you want to use direct access mode (mapped drive or UNC path), you will need to manually assign users the required file system rights to their post office directories. For instructions, see "Granting File System Rights to the Post Office Directory" on page 1069.
- **GroupWise Software Distribution Directory:** If you want users to have file system rights to a GroupWise software distribution directory to install or run the GroupWise client, you will need to manually assign rights. For instructions, see "Granting File System Rights to the Software Distribution Directory" on page 1071.
- **Mailbox Backup Directory:** For users to restore their mailbox from a network backup directory, they need the appropriate file system rights to the directory. For more information, see "Granting File System Rights to the Mailbox Backup Directory" on page 1071.

Granting File System Rights to the Post Office Directory

The following information applies only to users who are running the GroupWise client in direct access mode. Users who are running in client/server access mode do not require rights to the post office directories.

To increase security in your post office directories, you should restrict rights as shown in the following table.

Directories	NetWare Rights	Windows NT Permissions
post office	RWC--F	Change
agents	------	No Access
nlm	------	No Access
language	------	No Access
nt	------	No Access
language	------	No Access
gwdms	RW---F	Change
lib*x*	RW---F	Change
index	RW---F	Change
archive	RW---F	Change
ar*xx*	RW---F	Change
docs	RWCEMF	Full Control
fd*x*	RWCEMF	Full Control
offiles	R----F	Change
fd*x*	RWCEMF	Full Control
ofmsg	RWCEMF	Full Control
ofuser	RWCEMF	Full Control
index	RW---F	Change
ofviews	------	No Access
win	R----F	Read
ofwork	R----F	Read
ofdirect	RWCEMF	Full Control
wpcsin	RWCEMF	Full Control
0-7	-WC-M-	Change
problem	-WC-M-	Change
wpcsout	------	No Access
ads	------	No Access
0-7	------	No Access
chk	RWCEMF	Full Control
0-3	-WC-M-	Change

Directories	NetWare Rights	Windows NT Permissions
defer	-WC-M-	Change
ofs	RWC-MF	Full Control
0-7	RWC-MF	Full Control
problem	-WC-M-	Change

Granting File System Rights to the Software Distribution Directory

The software distribution directory contains the GroupWise client for Windows. To set up and run the GroupWise client, users require the directory rights listed in the table below.

Directories	NetWare Rights	Windows Permissions
software distribution directory	R----F	Read
admin	------	No Access
agents	------	No Access
client	R----F	Read
ofviews	R----F	Read
win32	R----F	Read
internet	------	No Access
domain	------	No Access
po	------	No Access

IMPORTANT: Users require rights only to the client directory and subdirectories. The other directories (admin, agents, domain, internet, and po) are administration directories that users should not have access to.

Granting File System Rights to the Mailbox Backup Directory

If you've backed up a user's network mailbox, or a user has backed up his or her local mailbox, to a network location, the user requires Read and Write file system rights to the backup directory in order to restore his or her mailbox.

87 Spam Protection

Unwanted Internet e-mail messages (spam) can be a distracting nuisance to GroupWise® client users. Your first line of defense against spam is the Internet Agent. Your second line of defence is the Junk Mail Handling feature of the GroupWise Windows client.

- "Configuring the Internet Agent for Spam Protection" on page 1073
- "Configuring the GroupWise Client for Spam Protection" on page 1073

Configuring the Internet Agent for Spam Protection

In ConsoleOne®, you can configure the Internet Agent to reject messages in certain situations:

- Messages are received from known open relay hosts or spam hosts (Internet Agent object > Access Control tab > Blacklists page).
- Messages are received from any hosts that you specifically do not want to receive messages from (Internet Agent object > Access Control tab > edit the default class of service > set Allow Incoming Messages, prevent Incoming Messages, and Exceptions as needed).
- Thirty messages are received within 10 seconds from the same sending host (Internet Agent object > SMTP/MIME Settings tab > Security Settings page). The number of message and the time interval can be modified to identify whatever you consider to be a potential mailbomb.
- Messages are received from SMTP hosts that are not using the AUTH LOGIN host authentication method (/forceinboundauth startup switch).
- The sender's identify cannot be verified (Internet Agent object > SMTP/MIME Settings tab > Security Settings page).

For detailed setup instructions on these anti-spam security measures, see Chapter 51, "Blocking Unwanted E-Mail," on page 719.

Messages that are identified as spam by the Internet Agent are not accepted into your GroupWise system.

Configuring the GroupWise Client for Spam Protection

The Junk Mail Handling feature in the GroupWise client is enabled by default, although you can control its functionality in ConsoleOne (Domain, Post Office, or User object > Tools menu > GroupWise Utilities > Client Options > Environment > General tab).

The Junk Mail Handling feature provides users with the following options for dealing with unwanted messages that have not been stopped by the Internet Agent:

- Individual e-mail addresses or entire Internet domains can be placed on the user's Block List. Messages from blocked addresses never arrive in the user's mailbox.

- Individual e-mail addresses or entire Internet Domains can be placed on the user's Junk List. Messages from these addresses are automatically delivered to the Junk Mail folder in the user's mailbox. The user can configure automatic deletion of items in the Junk Mail folder and can also create rules to act on items placed in the Junk Mail folder.
- Messages from users whose addresses are not in the user's personal address books can be automatically delivered to the Junk Mail folder.

For detailed usage instructions for the Junk Mail Handling feature in the GroupWise client, see "Handling Unwanted Mail" in "Working with Items in Your Mailbox" in the *GroupWise 6.5 Windows Client User Guide*.

The Junk Mail Handling feature is not available in the GroupWise WebAccess client.

88 Virus Protection

Virus protection for your GroupWise® system is provided by third-party products, including:

- GWAVA* by Beginfinite*
- RAV* AntiVirus* by GeCAD Software*
- IronMail* by CipherTrust*
- GWGuardian* by The Messaging Architects*

For information about these security products for use with your GroupWise system, see the Partner Product Guide (http://www.novell.com/partnerguide/).

XVI Documentation Updates

This section lists updates to the *GroupWise 6.5 Administration Guide* that have been made since the initial release of GroupWise® 6.5. The information will help you to keep current on documentation updates and, in some cases, software updates (such as a Support Pack release).

The information is grouped according to the date when the *GroupWise 6.5 Administration Guide* was republished. Within each dated section, the updates are listed by the names of the main table of contents sections.

The *GroupWise 6.5 Administration Guide* has been updated on the following dates:

February 6, 2006 (GroupWise 6.5 SP6)

Location	Change
System	
"Client Languages" on page 103	Explained that the GroupWise client user guides are not translated into all of the languages into which the software is translated and linked to a list of languages in which the client user guides are available.
Post Offices	
"Restricting the Size of Messages That Users Can Send" on page 175	Added information about message size restrictions between your GroupWise system and the Internet.
Databases	

Location	Change
"Starting GWCheck on a Linux Workstation" on page 394	Indicated that the GWCheck RPM is available in the /client subdirectory as well as the /admin subdirectory of your software distribution directory.
Post Office Agent	
"Restricting Message Size between Post Offices" on page 455	Explained what happens if the message exceeds the limit; added a link to other methods of message size restriction.
Message Transfer Agent	
"Restricting Message Size between Domains" on page 588	Explained what happens if the message exceeds the limit; added a link to other methods of message size restriction.
"Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways" on page 636	Indicated that gateways are also affected by the MTA scan cycle settings.
Internet Agent	
"Creating a Class of Service" on page 706	Explained what happens if the message exceeds the limit; added a link to other methods of message size restriction.
"/defaultcharset" on page 780	Included examples where the character set name includes hyphens (-).
WebAccess Agent	
"Assigning a Default WebAccess Agent to a Post Office" on page 815	Added information about how this setting is used to select an appropriate default WebAccess Agent for a post office.
"Assigning a Default WebAccess Agent to a Domain" on page 816	Added information about how this setting is used to select an appropriate default WebAccess Agent for a domain.
"/http" on page 897	Updated the syntax for the /http startup switch. Prior to Support Pack 5, this switch enabled HTTP using 7211 as the default port number. Starting in Support Pack 5, you must specify the port number.
Client	
"Send Options: Disk Space Management" on page 995	Added a link to other methods of message size restriction.
Security	
"Manually Granting eDirectory Rights" on page 1068	Made corrections to the rights table to list the properties associated with the POA object.

October 31, 2005

Location	Change
System	
"Import" on page 68 and "Export" on page 71	Updated the location where you can download the Import/Export utility.
Users	
"Disabling and Enabling GroupWise Accounts" on page 214	Explained that, after a GroupWise account has been disabled, proxy users can still access it.
Databases	
"Using DBCopy on Linux Servers" on page 412	Corrected the path to the dbcopy executable; added the -l switch.
Internet Agent	
"Configuring POP3/IMAP4 Services" on page 684	Compared POP3 capabilities of the Internet and the POA.
"Using Paging" on page 689	Corrected the pager e-mail address so that the /l and /b switches follow the address.
Client	
"Setting Client Options" on page 976	Clarified that setting a lock on an option setting at a higher level such as a post office overrides that option setting at a lower level such as a user.

September 19, 2005 (GroupWise 6.5 SP5)

Location	Change
System	
Chapter 1, "GroupWise System Administration," on page 33	Added an overview of GroupWise administration.
Chapter 2, "ConsoleOne Administration Tool," on page 35	Added an overview of ConsoleOne®, including how to install and start it on Windows and Linux.
Chapter 6, "GroupWise Addressing," on page 81	Consolidated sections related to addressing into a single section.
"Nickname Overrides" on page 96	Explained how you can now configure Internet addressing on nicknames.

Location	Change
Chapter 7, "Multilingual GroupWise Systems," on page 103	Added a new section for non-English GroupWise administrators.
Domains	
"Converting a Secondary Domain to a Primary Domain" on page 126	Added a step for connecting to the primary domain before performing the conversion.
"Deleting a Domain" on page 128	Added a step for connecting to the primary domain before deleting the domain. Added a step for stopping the MTA and uninstalling the agent software if applicable.
Post Offices	
"Deleting a Post Office" on page 184	Added a step for stopping the POA and uninstalling the agent software if applicable.
Users	
"Creating a Nickname for a User" on page 213	Removed the incorrect information that nicknames are not valid Internet addresses. Internet users can address a message to *nickname@host*.
Distribution Lists, Groups, and Organizational Roles	
"Deleting a Distribution List" on page 244	Provided steps for deleting multiple distribution lists in the same post office.
"Removing a Group from GroupWise" on page 254	Corrected the instructions. It is possible to remove a group from GroupWise without deleting it from eDirectoryTM.
"Removing an Organizational Group from GroupWise" on page 259	Corrected the instructions. It is possible to remove an organization group from GroupWise without deleting it from eDirectory.
Databases	
Chapter 31, "Backing Up GroupWise Databases," on page 375	Improved backup instructions for Linux and Windows users.
"GroupWise Check" on page 391	Added a link to GroupWise Check error codes.
"Starting GWCheck on a Windows Workstation" on page 393	Explained how to get the Repair Mailbox item to appear on the Tools menu in the GroupWise Windows client.
"Executing GWCheck from a Windows Batch File" on page 398	Added the /pa switch.
"Executing GWCheck from a Linux Script" on page 398	Added the --pa switch.

Location	Change
"GWTSA Functionality" on page 399	Added the ofmsg directory to the list of directories that the GWTSA backs up.
Post Office Agent	
"Enhancing Post Office Security with SSL Connections to the POA" on page 458	Specified the default location for SSL certificate files and key files.
"Providing LDAP Server Configuration Information" on page 461	Corrected the information about using SSL connections between the POA and LDAP servers.
Internet Agent	
"Setting Up Paging" on page 688	Added two missing steps.
/flatfwd	Improved the explanation of the switch.
Monitor	
Chapter 65, "Starting the Monitor Agent," on page 903	Noted that you do not need to be logged in as root to start the Monitor Agent on Linux. Added instructions for stopping the Monitor Agent on Linux and Windows.
"Understanding the Monitor Agent Consoles" on page 906	Added a general comparison of the Monitor Agent consoles.
Chapter 70, "Comparing the Monitor Agent Consoles," on page 953	Added more detail to the Monitor Agent console comparison table.
Client	
"LaunchMessenger=" on page 1006	Added a section to the setup.cfg file configuration on how to launch GroupWise Messenger.
Security	
"Bypassing Mailbox Passwords to Respond to Corporate Mandates" on page 1036	Tied in information about trusted applications.

February 28, 2005 (GroupWise 6.5 SP4)

Location	Change
System	
"System Operations" on page 43	Explained what you would see when connected to a secondary domain if Restrict System Operations to Primary Domain is selected under System Preferences.

Location	Change
Post Offices	
"Auditing Mailbox License Usage in the Post Office" on page 180	Indicated that the process of auditing mailbox license usage can be added to a POA scheduled event.
Users	
"Moves Between GroupWise 6.x Post Offices" on page 199	Clarified that client option settings are typically not lost when a user's mailbox is moved from one post office to another.
"Removing GroupWise Accounts" on page 215	Noted that when a GroupWise account is deleted, the user's personal databases (such as an archive, a Caching mailbox, or a Remote mailbox) are not affected.
Databases	
"Maintaining Domain and Post Office Databases" on page 345, "Maintaining User/Resource and Message Databases" on page 353, and "Maintaining Library Databases and Documents" on page 359	Explained that damage to databases cannot be prevented but generally can be repaired by the GroupWise database maintenance tools.
"Setting Up a Restore Area" on page 381	Clarified that, if you specify a new directory as a restore area, ConsoleOne does not create the directory when it creates the Restore Area object. It is the Target Service Agent that performs the restore that creates the new directory.
Post Office Agent	
"Scheduling Database Maintenance" on page 467 and "Scheduling Disk Space Management" on page 469	Explained that you cannot create or edit a POA scheduled event if you are connected to a secondary domain and Restrict System Operations to Primary Domain is selected under System Preferences.
Message Transfer Agent	
"Using MTA Startup Switches" on page 643	Removed the /queuethreshold startup switch.
Internet Agent	
"Classes of Service" on page 705	Improved the explanation of the default class of service and emphasized that the message size limit set in the default class of service is treated as the GroupWise system message size limit for incoming messages from the Internet.
"Blocked.txt File" on page 721	Clarified that wildcard characters can be used in hostnames as well as IP addresses in the blocked.txt file. There is no size limit on the blocked.txt file.
/dontreplaceunderscore,	Clarified the usage of the /dontreplaceunderscore startup switch.
Monitor	

Location	Change
"Using Monitor Agent Switches" on page 957	Added some switches that were missing from the list.
Client	
"Distributing the GroupWise Client" on page 1003	Moved the SetupIP information out of its own section and into this section, along with the other client software distribution methods, to make it easier to find.
"Supporting the GroupWise Client in Multiple Languages" on page 1021	Added instructions for supporting GroupWise in a multilingual environment.
Security	
"Generating a Certificate Signing Request and Private Key" on page 1041	Added examples of Linux paths with certificate and key filenames.
"Creating Your Own Certificate" on page 1043	Indicated that on Linux, the Certificate Server snap-in to ConsoleOne is installed by default. Noted that you can use iManager as well as ConsoleOne to create server certificates.

November 30, 2004 (GroupWise 6.5 SP3)

Location	Change
Databases	
"Running GWTSA" on page 400	Clarified the GWTSA command with improved examples.
"NetWare Target Service Agent for File Systems" on page 403	Introduced the improved capabilities of the NetWare Target Service Agent for File Systems (TSAFS) for backing up GroupWise.
"GroupWise Time Stamp Utility" on page 405	Noted that the Time Stamp (GWTMSTMP) utility is not needed when using TSAFS to back up a GroupWise 6.5 system where Support Pack 3 has been installed.
Post Office Agent	
"Controlling Client Redirection Inside and Outside Your Firewall" on page 458	Added instructions for controlling client redirection.
"/imapreadlimit" on page 533	Added a new startup switch.
"/ip" on page 535	Clarified that the IP address specified by the /ip switch is associated with all POA ports (HTTP, IMAP, and so on).
Internet Agent	
"Creating a Class of Service" on page 706	Explained how to create an entry in the Allow Messages From list for messages where the username is blank.

Location	Change
"Using Internet Agent Log Files" on page 746 and "Log File Switches" on page 800	Changed the log file naming convention from *mmdd*log.*nnn* to *mmdd*gwia.*nnn*, which distinguishes Internet Agent log files from other agent log files.
"/dontreplaceunderscore" on page 778, "/keepsendgroups" on page 779, and "/imapreadlimit" on page 794	Added new startup switches.
Security	
"Requiring GroupWise Passwords" on page 1034	Added Caching mode in the Cross-Platform client to the list of circumstances where a GroupWise password is required.

September 30, 2004

Location	Change
System	
"Trusted Applications" on page 62	Pointed out that trusted applications rely on the MTA for message transfer.
"Override Options" on page 91	Clarified how to handle e-mail addresses that are not being processed correctly in the selected address format.
Users	
"Monitoring User Move Status" on page 203	Added the Retry Mailbox Item Retrieval status.
"Creating a Nickname for a User" on page 213	Emphasize that a nickname must be unique.
Distribution Lists	
"Adding Members to a Distribution List" on page 242	Explained the difference between distribution lists and shared groups in the client.
"Adding External Users to a Distribution List" on page 248	Explained how to add external users to a distribution list.
Databases	
"Gathering Mailbox Statistics" on page 367	Explained how to sent mailbox statistics to users in addition to the administrator.
"GWTSA Functionality" on page 399	Clarified that the GWTSA supports whatever backup capabilities are available in the backup software with which it is used.
Post Office Agent	

Location	Change
"Adjusting the POA Logging Level and Other Log Settings" on page 446 and "/loglevel" on page 542	Clarified the verbose logging does not degrade POA performance.
Message Transfer Agent	
"Adjusting the MTA Logging Level and Other Log Settings" on page 588 and "/loglevel" on page 652	Clarified the verbose logging does not degrade MTA performance.
Internet Agent	
"Using Internet Agent Log Files" on page 746	Clarified the verbose and diagnostic logging does not degrade Internet Agent performance.
"Alphabetical List of Switches" on page 767	Corrected the spelling of the /noesmtp switch.
WebAccess Agent	
"Blocked.txt File" on page 721	Added examples of IP address ranges for use in the blocked.txt file
"Controlling WebAccess Agent Logging" on page 832 and "/loglevel" on page 898	Clarified the verbose and diagnostic logging does not degrade WebAccess Agent performance
Monitor	
"Configuring Proxy Service Support for the Monitor Web Console" on page 925	Added instructions for configuring the Monitor Agent and Monitor Web console to support proxy service through a firewall.
"Configuring Monitor Agent Log Settings" on page 925	Clarified the verbose and diagnostic logging does not degrade Monitor Agent performance
Client	
"Custom Views" on page 983	Noted that custom views cannot be created in GroupWise but are used by third-party products.
Security	
"Creating Your Own Certificate" on page 1043	Added instructions for generating a public certificate in ConsoleOne.

June 25, 2004 (GroupWise 6.5 SP2 and GroupWise 6.5 for Linux SP2)

Location	Change
Databases	

Location	Change
“GroupWise Database Copy Utility” on page 412	Indicated that DBCopy can now copy domains as well as post offices.
Message Transfer Agent	
“/lrwaitdata” on page 652	Added a new startup switch.
Internet Agent	
/defaultcharset /popintruderdetect /realmailfrom	Added some new startup switches.
WebAccess	
“Configuring User Access to WebAccess Features” on page 826	Updated the URL for information about Stellent viewers.

May 3, 2004 (GroupWise 6.5 for Linux)

Location	Change
System	
Chapter 3, “GroupWise View,” on page 37	Mentioned that the screen shots in the *GroupWise 6.5 Administration Guide* are from the Windows version of ConsoleOne, but the Linux version offers the same functionality.
“System Preferences” on page 44	Explained the new Linux Settings tab in the GroupWise System Preferences dialog box in ConsoleOne.
“Select Domain” on page 43	Explained that, in the Linux version of ConsoleOne, UNC paths are interpreted with the first item in the path being the Linux server and subsequent items being directories in the path.
“System Preferences” on page 44	Explained the mount directory system preference available in the Linux version of ConsoleOne.
“Import” on page 68 and “Export” on page 71	Indicated that the Import/Export utility is not available on Linux.
“Check eDirectory Schema (Linux Only)” on page 73	Added the Check eDirectory Schema utility available in the Linux version of GroupWise.
Domains	
“Choosing the Domain Name” on page 114	Clarified that domain names cannot contain asterisks (*).
“Deciding Where to Create the Domain Directory” on page 114	Pointed out that domains can now be located on Linux servers and that domain directory names must consist of lowercase letters.

Location	Change
"MTA Access to New Post Offices: Mapped and UNC Links vs. TCP/IP Links" on page 116	Mentioned that the Linux MTA requires TCP/IP links to the POA.
Post Offices	
"Choosing the Post Office Name" on page 151	Clarified that post office names cannot contain asterisks (*).
"Deciding Where to Create the Post Office Directory" on page 152	Pointed out that post offices can now be located on Linux servers and that post office directory names must consist of lowercase letters.
"Managing Disk Space Usage in the Post Office" on page 171	Explained that the Cross-Platform client does not currently respect mailbox size limits set in ConsoleOne.
"Auditing Mailbox License Usage in the Post Office" on page 180	Added the Cross-Platform client to the list of programs that require a full client license.
Resources	
"Creating a New Resource" on page 224	Clarified that resource names cannot contain asterisks (*).
Distribution LIsts and Groups	
"Creating a New Distribution List" on page 239	Clarified that distribution list names cannot contain asterisks (*).
Libraries and Documents	
"Libraries" on page 263	Pointed out that you cannot list libraries or select a default library in the Cross-Platform client.
"Document Properties" on page 265	Pointed out that document properties cannot be displayed in the Cross-Platform client.
"Document Properties" on page 265	Pointed out that you cannot create new documents in the Cross-Platform client.
"Document Properties" on page 265	Pointed out that you cannot configure document properties in ConsoleOne on Linux. However, you can use the Windows version of ConsoleOne to configure document properties for libraries located on Linux.
"Choosing the Library Name" on page 270	Clarified that library names cannot contain asterisks (*).
Databases	
"Backing Up a Post Office" on page 375	Recommended using the GroupWise Database Copy utility (DBCopy) to assist with backing up post offices on Linux.
"Restoring Deleted Mailbox Items" on page 381	Pointed out that the Cross-Platform client cannot access a restore area.

Location	Change
"Starting GWCheck on a Linux Workstation" on page 394 and "Executing GWCheck from a Linux Script" on page 398	Explained how to use GWCheck on Linux.
"GroupWise Time Stamp Utility" on page 405	Pointed out that GWTMSTMP is not available on Linux.
"GroupWise Database Copy Utility" on page 412	Explained how to use DBCopy on Linux.
Post Office Agent	
"Post Office Access Mode" on page 422	Mentioned that the Cross-Platform client requires a TCP/IP connection to the POA.
"Client/Server Processing" on page 423	Pointed out that Remote mode is not available in the Cross-Platform client.
"Cross-Platform Issues in the Post Office" on page 425	Added Linux and Macintosh to the list of platform alternatives.
"POA/Post Office Platform Dependencies Because of Direct Access Requirements" on page 426	Updated the cross-platform matrix with Linux information.
"Starting the Linux POA" on page 433	Added information about starting the Linux POA.
"Uninstalling the Linux POA" on page 436	Added information about uninstalling the Linux POA.
"Adjusting the POA for a New Post Office Location" on page 445	Added information about the Linux POA startup file.
"Using Client/Server Access to the Post Office" on page 447	Updated the information about the default number of physical and application connections.
"Simplifying Client/Server Access with a GroupWise Name Server" on page 449	Added information about modifying DNS on Linux servers.
"Configuring Trusted Application Support" on page 466	Added information about configuring the POA to support trusted applications.
"Monitoring the POA from the POA Agent Console" on page 475	Explained that the --show switch is required in order to display the Linux POA agent console.
"Stopping the POA" on page 480	Added information about stopping the Linux POA when it is running in the background as a daemon.

Location	Change
"Checking the POA Operating System Environment" on page 493	Added information about the Linux POA Web console Environment page.
"Setting Up SNMP Services for the Linux POA" on page 500	Added steps for setting up SNMP on Linux.
"Copying and Compiling the POA MIB File" on page 502	Explained where to find the POA MIB file.
"Using Platform-Specific POA Monitoring Tools" on page 505	Added Linux monitoring tools.
"Adjusting the Number of POA Threads for Client/Server Processing" on page 507	Updated the information about adjusting the number of POA TCP handler threads.
"Adjusting the Number of Connections for Client/Server Processing" on page 508	Updated the information about adjusting the number of physical and application connections.
Chapter 40, "Using POA Startup Switches," on page 523	Added Linux switches to the list of POA startup switches.
"@filename" on page 526	Added information about the Linux POA startup file.
"/log" on page 541	Added information about the Linux POA log file.
Message Transfer Agent	
"Cross-Platform Issues between Domains and Post Offices" on page 561	Added Linux to the list of platform alternatives.
"MTA Platform Dependencies Because of Direct Access Requirements to Post Offices" on page 562	Updated the domain to post office cross-platform matrix with Linux information.
"MTA Platform Dependencies Because of Direct Access Requirements to the Domain" on page 562	Updated the domain to domain cross-platform matrix with Linux information.
"Starting the Linux MTA" on page 570	Added information about starting the Linux MTA.
"Uninstalling the Linux MTA" on page 573	Added information about uninstalling the Linux MTA.

Location	Change
“Changing the Link Protocol between Domains” on page 579 and “Changing the Link Protocol between a Domain and Its Post Offices” on page 583	Pointed out that TCP/IP links are required between domains and post offices on Linux.
“Adjusting the MTA for a New Location of a Domain or Post Office” on page 587	Added information about the Linux MTA startup file.
“Enabling eDirectory User Synchronization” on page 599	Added steps for setting up eDirectory user synchronization for the Linux MTA
“Monitoring the MTA from the MTA Agent Console” on page 605	Explained that the --show switch is required in order to display the Linux MTA agent console.
“Stopping the MTA” on page 609	Added information about stopping the Linux MTA when it is running in the background as a daemon.
“Checking the MTA Operating System Environment” on page 620	Added information about the Linux MTA Web console Environment page.
“Setting Up SNMP Services for the Linux MTA” on page 628	Added steps for setting up SNMP on Linux.
“Copying and Compiling the MTA MIB File” on page 630	Explained where to find the MTA MIB file.
“Using Platform-Specific MTA Monitoring Tools” on page 633	Added Linux monitoring tools.
Chapter 46, “Using MTA Startup Switches,” on page 643	Added Linux switches to the list of MTA startup switches.
“@filename” on page 645	Added information about the Linux MTA startup file.
“/log” on page 651	Added information about the Linux MTA log file.
Internet Agent	
“Modifying Log Settings in ConsoleOne” on page 747	Added the location for Internet Agent log files on Linux.
“How to Use Startup Switches” on page 765	Added the location for the Internet Agent configuration files (gwia.cfg) on Linux.
/nomappriority /killthreads /ldapserverport /smtpport /xspam	Added new Internet Agent startup switches.

Location	Change
WebAccess	
“Installing Additional Components on Linux” on page 809	Added WebAccess installation instructions for Linux.
“Specifying a WebAccess Agent in the WebAccess URL” on page 813	Added the WebAccess URL for Linux.
“Modifying WebAccess Settings” on page 829	Added the WebAccess default disk cache path for Linux.
“Controlling the Agent’s Logging” on page 832	Added Linux to the table of WebAccess logging information.
“Modifying Log Settings in ConsoleOne” on page 833	Added the default location for WebAccess Agent log files on Linux.
“Modifying Log Settings through Startup Switches” on page 834	Added the location of the WebAccess Agent startup file for Linux.
“Automating Reattachment to NetWare Servers” on page 839	Added the location of the default WebAccess temporary directory on Linux.
“Adding or Removing Service Providers” on page 844	Mentioned that, on Linux, WebAccess includes a third service provider, the WebAccessDocumentProvider.
Monitor	
“Starting the Linux Monitor Agent” on page 903	Added instructions for starting the Linux Monitor Agent.
Chapter 66, “Configuring the Monitor Agent,” on page 909 and Chapter 67, “Using the Monitor Agent Console,” on page 927	Clarified that the Monitor Agent console is available only on Windows, not on Linux.
“Displaying the Monitor Web Console” on page 947	Added the URL for displaying the Monitor Web console on Linux.
Chapter 71, “Creating a PQA File for the Monitor Web Console,” on page 955	Clarified that a PQA file for the Monitor Web console can be created on Windows, but not on Linux.
Chapter 72, “Using Monitor Agent Switches,” on page 957	Added information about the Linux Monitor Agent configuration file and startup switches.
Client	
“GroupWise Modes” on page 965	Noted that Remote mode is not available in the Cross-Platform client.

Location	Change
"Allowing or Forcing Use of Caching Mode" on page 966	Emphasized the need for manual backups if the administrator forces Caching mode on Cross-Platform client users.
"Accounts Menu" on page 972	Noted that the Accounts menu where you set up POP3, IMAP4, and NNTP accounts is not available in the Cross-Platform client.
"Client Options Summary" on page 973	Indicated which client options are recognized by the Cross-Platform client.
"Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client" on page 1003	Noted that SetupIP and AutoUpdate do not apply to the Cross-Platform client.
"Using Red Carpet to Distribute the GroupWise Cross-Platform Client" on page 1020	Pointed out that Red Carpet can be used to distribute the Cross-Platform client software.
"Using GroupWise Check with the Cross-Platform Client" on page 1024	Explained how Cross-Platform client users can use GroupWise Check on Linux and noted that GroupWise Check is not available on Macintosh.
Chapter 78, "Startup Switches for the GroupWise Client," on page 1025	Marked which startup switches are not available in Cross-Platform client.
Security	
"Generating a Certificate Signing Request and Private Key" on page 1041	Explained how to start the GroupWise Generate CSR utility (gwcsrgen) on Linux.

October 31, 2003

Location	Change
Users	
"Checking GroupWise Account Usage" on page 214	Added links to information about identifying unused GroupWise accounts and measuring message traffic from individual GroupWise mailboxes.
Databases	
"Gathering Mailbox Statistics" on page 367	Updated the Expire Statistics options.
"Reducing the Size of User and Message Databases" on page 369	Updated the Expire/Reduce options.
Chapter 32, "Restoring GroupWise Databases from Backup," on page 379	Updated the bulleted list with the last item, which had been missing

Location	Change
Post Office Agent	
"Scheduling Disk Space Management" on page 469	Updated the Expire/Reduce options.
Internet Agent	
"Using Extended SMTP (ESMTP) Options" on page 663	Added information about supported ESMTP extensions.
"Customizing MIME Preamble Text" on page 678	Made a correction to give the file size in bytes, not kilobytes.
Client	
"Setting Client Options" on page 976	Indicated that user settings override post office settings, and post office settings override domain settings.
"Enabling AutoUpdate" on page 1011	Added information about the setupip directory being on the *GroupWise 6.5 Client* CD.
"Setupip.fil File" on page 1004	Added information about the setupip directory being on the *GroupWise 6.5 Client* CD.
Security	
"Requiring GroupWise Passwords" on page 1034	Added external entities as a situation where GroupWise passwords are required.
"Synchronizing GroupWise Passwords and LDAP Passwords" on page 1036	Explained that the equivalent of password synchronization between GroupWise and eDirectory™ can be accomplished using LDAP authentication.
"Using LDAP Passwords Instead of GroupWise Passwords" on page 1036	Clarified that GroupWIse passwords are sometimes required even when LDAP authentication is enabled, and provided steps for changing both GroupWise passwords and LDAP passwords in the GroupWise client.

July 16, 2003 (GroupWise 6.5 SP1)

Location	Change
System	
“Editing a Trusted Application” on page 62	Added information about the new Provides Message Retention Service setting that is required if a trusted application is used to retain user messages (for example, by copying them from GroupWise databases to a storage medium).
“System Preferences” on page 44	Under Admin Preferences (step 2), documented the new Display DirXML Warnings setting. Under Admin Lockout Settings (step 7), documented the new Lock Out Older GroupWise Administration Snap-Ins settings.
“Wildcard Addressing Syntax” on page 102	Clarified information about the addressing syntax available for each of the wildcard addressing settings (Limit to Post Office, Limit to Domain, Limit to System, and Unlimited).
Domains	
“Deciding Where to Create the Domain Directory” on page 114	Clarified that you can create domains on NetWare® 4.2 and NetWare 3.12 servers, although you cannot run the agents on these versions of NetWare.
Chapter 8, “Creating a New Domain,” on page 109	Provided links for instructions about creating domains in a Novell® cluster and a Microsoft cluster.
Post Offices	
“Deciding Where to Create the Post Office Directory” on page 152	Clarified that you can create post offices on NetWare 4.2 and NetWare 3.12 servers, although you cannot run the agents on these versions of NetWare.
Chapter 11, “Creating a New Post Office,” on page 147	Provided links for instructions about creating post offices in a Novell cluster and a Microsoft cluster.
Users	
“Creating a Single GroupWise Account” on page 190	Documented that GroupWise mailbox IDs cannot contain periods.
“Educating Your New Users” on page 196	Included suggestions for helping new users get started with GroupWise.
Databases	
“Re-creating a User Database” on page 356	Clarified a limitation of using the Recreate User Database action of Mailbox/Library Maintenance, specifically that all folder assignments are lost, so that the user must completely reorganize his or her re-created mailbox.
“Recovering Deleted GroupWise Accounts” on page 384	Removed instructions for manually distribution list membership for a recovered GroupWise account. The Recover Deleted Account now handles this automatically.

Location	Change
Chapter 33, “Retaining User Messages,” on page 387	Documented GroupWise support for trusted applications that perform message retention services. When you enable message retention services for a user, the user is unable to purge or archive mailbox items until after the trusted application has copied the items from the user’s mailbox to another storage location.
“GWTSA Startup Switches” on page 403	Clarified that the /log switch turns on logging and displays a logging screen. The log file is created in the sys:\system\tsa directory.
“GroupWise Time Stamp Utility” on page 405	Added information about how to use the GroupWise Time Stamp utility to manually add backup, restore, and retention time stamps to user databases.
Post Office Agent	
Chapter 36, “Installing and Starting the POA,” on page 427	Provided links for instructions about installing the POA in a Novell cluster and a Microsoft cluster.
“Supporting CAP Clients” on page 451	Documented that you can configure the POA so that users of CAP clients can connect to their GroupWise mailboxes.
“Securing Client/Server Access through a Proxy Server” on page 456	Documented that you can now specify different numbers for the local intranet client/server port and the Internet proxy client/server port. Documented that the POA Web console now lists proxy server addresses and ports along with POA server addresses and ports.
“Performing Nightly User Upkeep” on page 472	Explained how to generate the downloadable system Address Book for Remote client users between the regular once-daily cycles.
“Using NetWare 6.5 Remote Manager” on page 498	Added information about using NetWare Remote Manager to view the IP address and port numbers assigned to a POA running on a NetWare 6.5 server.
Message Transfer Agent	
Chapter 42, “Installing and Starting the MTA,” on page 565	Provided links for instructions about installing the MTA in a Novell cluster and a Microsoft cluster.
“Using NetWare 6.5 Remote Manager” on page 626	Added information about using NetWare Remote Manager to view the IP address and port numbers assigned to a MTA running on a NetWare 6.5 server.
Internet Agent	
“Understanding the Accounting File’s Fields” on page 717	Added information about the accounting file.
“Monitoring the Internet Agent through NetWare 6.5 Remote Manager” on page 744	Added information about using NetWare Remote Manager to view the IP address and port numbers assigned to an Internet Agent running on a NetWare 6.5 server.
WebAccess	

Location	Change
“Defining User Interfaces” on page 846	Documented the new Logout URL setting that enables you to define template-specific logout URLs for WebAccess in ConsoleOne rather than in the webacc.cfg file.
“Securing WebAccess Application Sessions” on page 850	Disable Caching: Documented the moving of the Disable Caching feature from the WebAccess Application object’s Templates page to the Security page. Also documented that the feature now controls Web browser caching in addition to proxy server caching. Single Sign-On: Clarified information about the password and username that must be included in a trusted server’s authentication header in order for single sign-on to work properly.
“Controlling Availability of WebAccess Features” on page 852	Added information about the new Maximum Document View Size feature.
“Defining User Interfaces” on page 862	Documented the new Logout URL setting that enables you to define template-specific logout URLs for WebPublisher in ConsoleOne rather than in the webpub.cfg file.
“Controlling Availability of WebPublisher Features” on page 865	Added information about the new Maximum Document View Size feature.
Chapter 60, “Customizing the WebAccess Interface,” on page 873	Documented the new customization.properties file that enables you to change the default logo and colors used in the WebAccess interface.
“Monitoring the WebAccess Agent through NetWare 6.5 Remote Manager” on page 881	Added information about using NetWare Remote Manager to view the IP address and port numbers assigned to a WebAccess Agent running on a NetWare 6.5 server.
Chapter , “Monitoring the WebAccess Application,” on page 882	Documented the new Web console for the WebAccess Application. The Web console enables you to use a Web browser to view information about the users currently logged in to WebAccess, view log file information, and view configuration information.
“/http” on page 897	Documented the /http switch that can be used to enable the WebAccess Agent’s Web console if it is not already enabled in ConsoleOne.
Client	
“Setting Client Options” on page 976	Added instructions for setting client options on multiple User objects at once.
“Environment Options: Retention” on page 986	Documented the new Retention option that was added as a GroupWise client Environment option.