# IX Post Office Agent

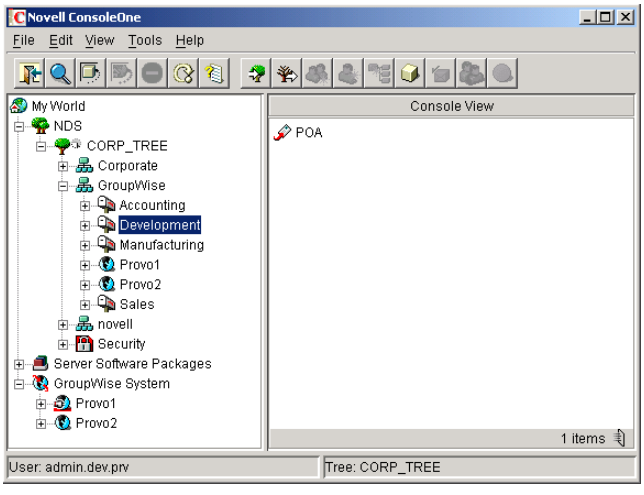
# 35 Understanding Message Delivery and Storage in the Post Office

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:

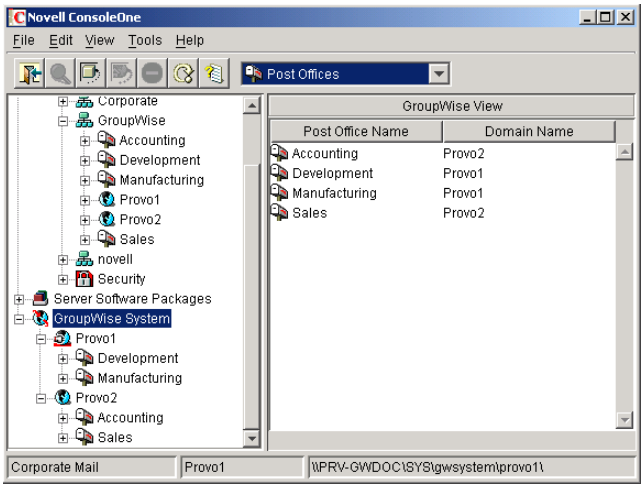


## Post Office Representation in ConsoleOne

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 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

Select the platform where you have installed the POA:



### 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

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] | | (required for message file processing) |
| Startup | 40 KB | See "Adjusting the Number of POA Threads for Message File Processing" on page 512. See also /threads. |
| Idle | 30 KB | |
| Processing | 2000 KB | |
| 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] | | (required for client/server processing) |
| Startup | 40 KB | See "Adjusting the Number of Connections for Client/Server Processing" on page 508. See also /tcpthreads. |
| Idle | 35 KB | |
| Processing | 2500 KB | |
| Client/server connections (each) | | (required for client/server processing) |
| No message processing | 45 KB | See "Adjusting the Number of Connections for Client/Server Processing" on page 508. See also /maxappconns and /maxphysconns. |
| Limited processing | 70 KB | |
| Heavy processing | 155 KB | |
| MTP processes | | (required for TCP/IP link with MTA) |
| Scanner/listener | 10 KB | See "Using TCP/IP Links between the Post Office and the Domain" on page 443. |
| Senders/receivers (each) | 5 KB | |
| QuickFinder™ thread | 30 KB | (required for indexing) |
| Building/updating indexes | 3000 KB | See "Regulating Indexing" on page 514. See also /qfinterval, /qfintervalinminute, /qfbaseoffset, /qfbaseoffsetinminute, and /noqf. |
| Compressing/combining indexes | 4000 KB | |
| 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 | | (required; occasional, temporary usage) |
| 25 events | 1530 KB | |
| 100 events | 2140 KB | |
| 365 events | 7885 KB | |
| Notify | 30 KB | (required) |

| POA Component | Approx. Memory | References |
|---|---|---|
| Admin thread | | (required for post office database update and repair) |
| Idle | 20 KB | |
| Processing | 125 KB | 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.

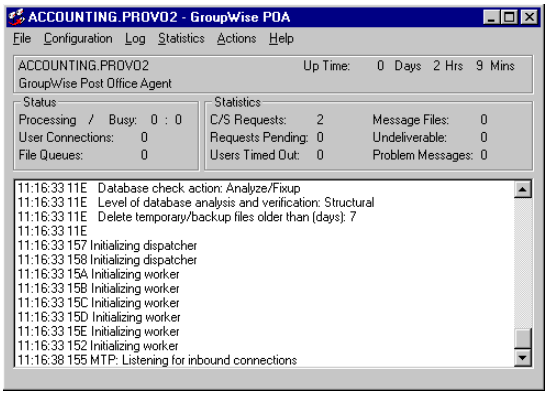
2. Enter the command to load the NetWare POA.

   **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.



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" on page 437
  - Creating a POA Object in eDirectory
  - Configuring the POA in ConsoleOne
  - Changing the Link Protocol between Post Office and Domain
  - Moving the POA to a Different server
  - Adjusting the POA for a New Post Office Location
  - Adjusting the POA Logging Level and Other Log Settings
- "Configuring User Access to the Post Office" on page 446
  - Using Client/Server Access to the Post Office
  - Simplifying Client/Server Access with a GroupWise Name Server
  - Supporting IMAP Clients
  - Supporting CAP Clients
  - Checking What GroupWise Clients Are in Use
  - Supporting Forced Mailbox Caching
  - Restricting Message Size between Post Offices
- "Configuring Post Office Security" on page 456
  - Securing Client/Server Access through a Proxy Server
  - Enhancing Post Office Security with SSL Connections to the POA
  - Providing LDAP Authentication for GroupWise Users
  - Enabling Intruder Detection
  - Configuring Trusted Application Support
- "Configuring Post Office Maintenance" on page 467
  - Scheduling Database Maintenance
  - Scheduling Disk Space Management
  - Performing Nightly User Upkeep

## 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:

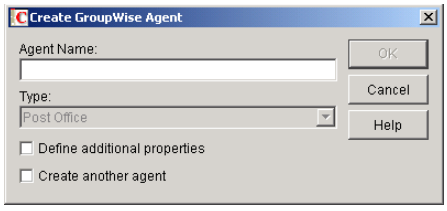
- "Creating a POA Object in eDirectory" on page 438
- "Configuring the POA in ConsoleOne" on page 439
- "Changing the Link Protocol between the Post Office and the Domain" on page 442
- "Moving the POA to a Different server" on page 445
- "Adjusting the POA for a New Post Office Location" on page 445

## 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.



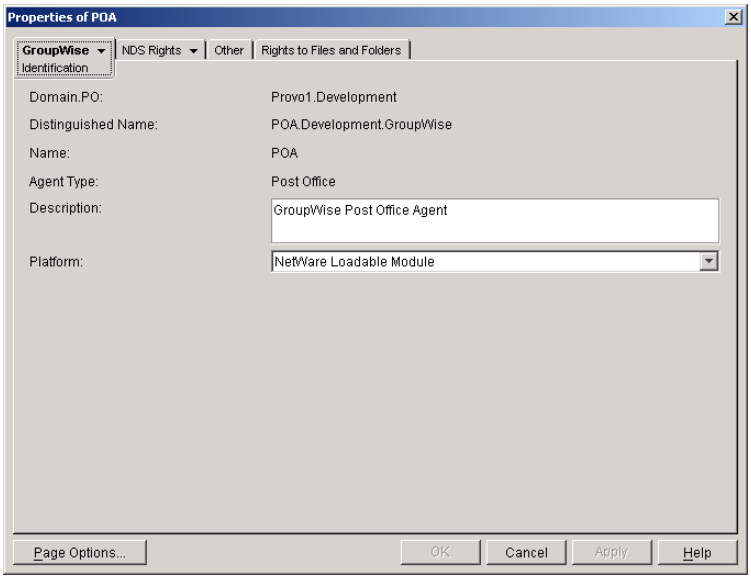

3. Type a unique name for the new POA. The name can include as many as 8 characters. Do not use any of the following invalid characters in the name:

| | |
|---|---|
| ASCII characters 0-13 | Comma , |
| Asterisk * | Double quote " |
| At sign @ | Extended characters |
| Braces { } | Parentheses ( ) |
| Colon : | 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.




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<br>Distinguished Name<br>Name<br>Type<br>Description<br>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.<br>See also /nomf, /nomfhigh, and /nomflow. |
| Message Handler Threads | See "Adjusting the Number of POA Threads for Message File Processing" on page 512.<br>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.<br>See also /notcpip. |
| TCP Handler Threads | See "Adjusting the Number of Connections for Client/Server Processing" on page 508.<br>See also /tcpthreads. |
| Max Physical Connections<br>Max Application Connections | See "Adjusting the Number of Connections for Client/Server Processing" on page 508.<br>See also /maxphysconns and /maxappconns. |
| Enable Caching | See /nocache. |
| CPU Utilization (NLM)<br>Delay Time (NLM) | See "Optimizing CPU Utilization for the NetWare POA" on page 520.<br>See also /cpu and /sleep. |
| Max Thread Usage for Priming and Moves | See "Supporting Forced Mailbox Caching" on page 454.<br>See also /primingmax. |
| Enable IMAP<br>Max IMAP Threads | See "Supporting IMAP Clients" on page 450.<br>See also /imap and /imapmaxthreads. |
| Enable CAP<br>Max CAP Threads | See "Supporting CAP Clients" on page 451.<br>See also /cap and /capmaxthreads. |
| Enable SNMP<br>SNMP Community "Get" String | See "Using SNMP Monitoring Programs" on page 499.<br>See also /nosnmp. |
| HTTP User Name<br>HTTP Password | See "Setting Up the POA Web Console" on page 489.<br>See also /httpuser and /httppassword. |
| **Network Address Page** | |
| TCP/IP Address<br>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.<br>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.<br>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.<br>See also /httpport and /httpssl. |
| Local Intranet Client/Server<br>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.<br>See also /port, /internalclientssl, and /externalclientssl. |
| IMAP | See "Supporting IMAP Clients" on page 450.<br>See also /imapport, /imapssl, and /imapsslport. |
| CAP | See "Supporting CAP Clients" on page 451.<br>See also /capport and /capssl. |
| **QuickFinder Page** | |
| Enable QuickFinder Indexing<br>Start QuickFinder Indexing<br>QuickFinder Interval | See "Regulating Indexing" on page 514 and "Configuring a Dedicated Indexing POA" on page 516.<br>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.<br>See also /gwchkthreads and /nogwchk. |
| Perform User Upkeep<br>Start User Upkeep<br>Generate Address Book for Remote<br>Start Address Book Generation | See "Performing Nightly User Upkeep" on page 472.<br>See also /nuuoffset, /nonuu, /rdaboffset, and /nordab. |
| Disk Check Interval<br>Disk Check Delay | See "Scheduling Disk Space Management" on page 469. |
| **POA Log Settings Page** | |
| Log File Path<br>Logging Level<br>Max Log File Age<br>Max Log Disk Space | See "Using POA Log Files" on page 497.<br>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<br>SSL Key File<br>Password | See "Enhancing Post Office Security with SSL Connections to the POA" on page 458.<br>See also /certfile, /keyfile, /keypassword. |
| **Post Office Settings Page** | |
| Remote User Name<br>Remote Password | See Chapter 36, "Installing and Starting the POA," on page 427.<br>See also /user and /password. |
| **Post Office Client Access Settings Page** | |
| Lock Out Older GroupWise Clients<br>Minimum Client Release Version<br>Minimum Client Release Date | See "Checking What GroupWise Clients Are in Use" on page 452.<br>See also /gwclientreleasedate, /gwclientreleaseversion, and /enforceclientversion. |
| Enable Intruder Detection<br>Incorrect Logins Allowed<br>Incorrect Login Reset Time<br>Lockout Reset Time | See "Enabling Intruder Detection" on page 465.<br>See also /intruderlockout, /incorrectloginattempts, /attemptsresetinterval, and /lockoutresetinterval. |
| **Post Office Security Page** | |
| LDAP Authentication | See "Providing LDAP Authentication for GroupWise Users" on page 461.<br>See also /ldapipaddr, /ldapport, /ldapuser, /ldappwd, /ldapuserauthmethod, /ldapdisablepwdchg, /ldapssl, /ldapsslkey, and /ldaptimeout.<br>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

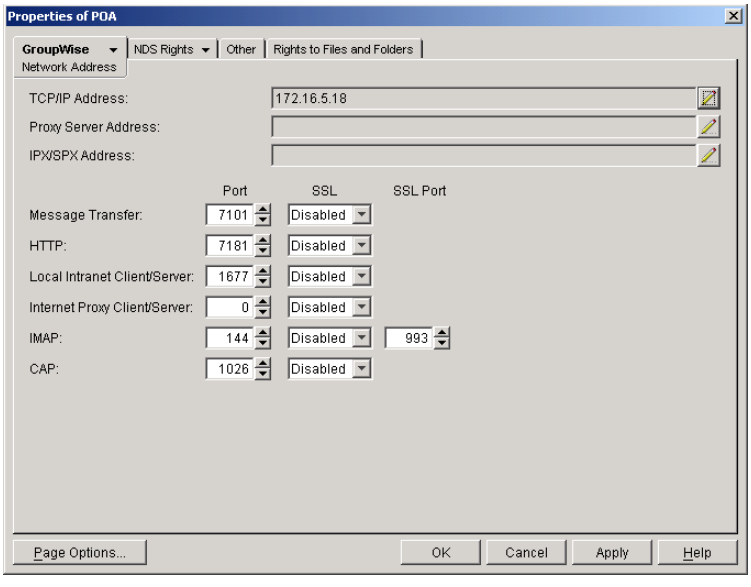
To change from a mapped or UNC link to a TCP/IP link between a post office and its domain, you must perform the following two tasks:

- "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.




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.

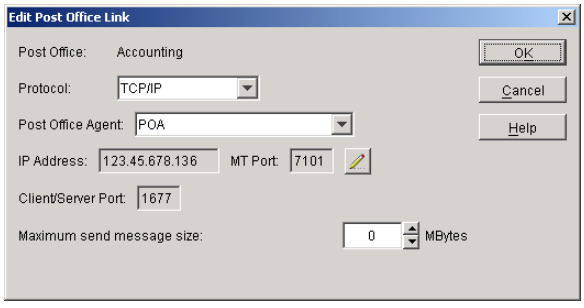
#### Changing the Link between the Post Office and the Domain to TCP/IP

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.




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.

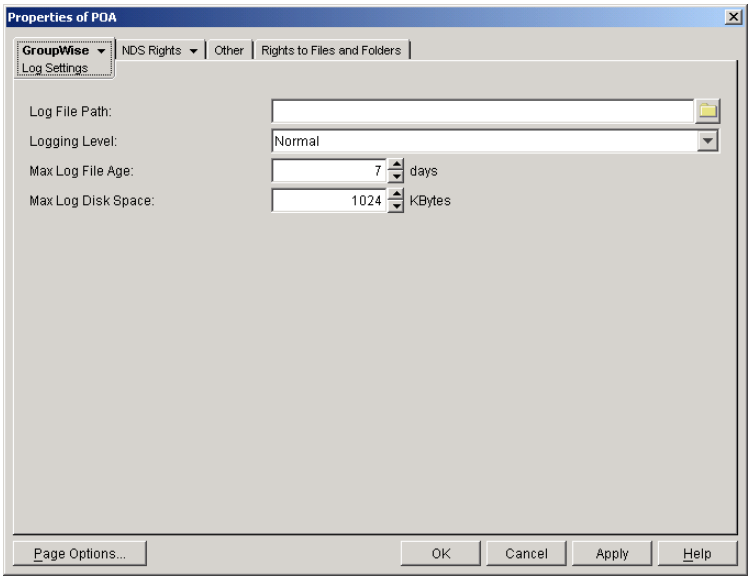
1. Stop the POA for the old post office location if it is still running.
2. Use an ASCII text editor to edit the POA startup file.

   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.




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

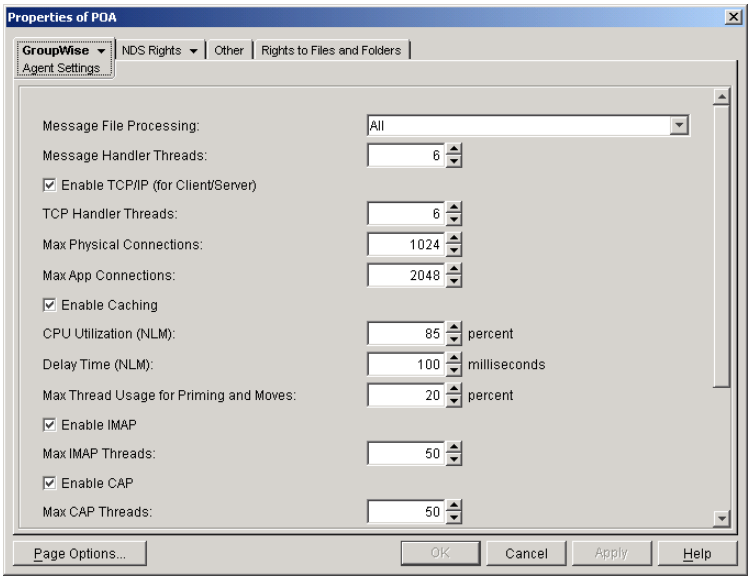
As described in "Post Office Access Mode" on page 422, the GroupWise 6.*x* client defaults to client/server access mode. The following topics help you configure the POA to customize the types of client/server access provided to the post office:

- "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:

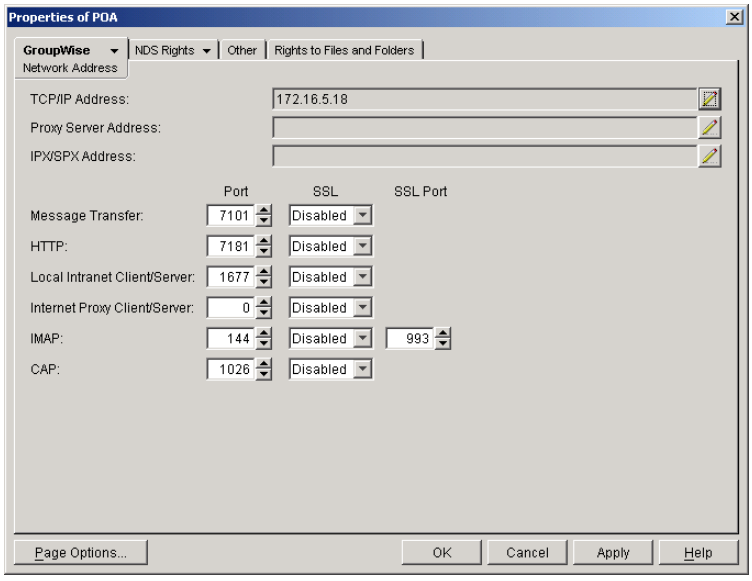
1. Make sure TCP/IP is properly set up on the server where the POA is running.
2. In ConsoleOne, browse to and right-click the POA object, then click Properties.
3. Click GroupWise > Agent Settings to display the Agent Settings page.



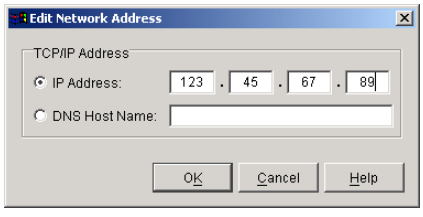

4. Make sure that Enable TCP/IP (for Client/Server) is selected.

   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.




6 On the Network Address page, click the pencil icon for the TCP/IP Address field to display the Edit Network Address dialog box.




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.

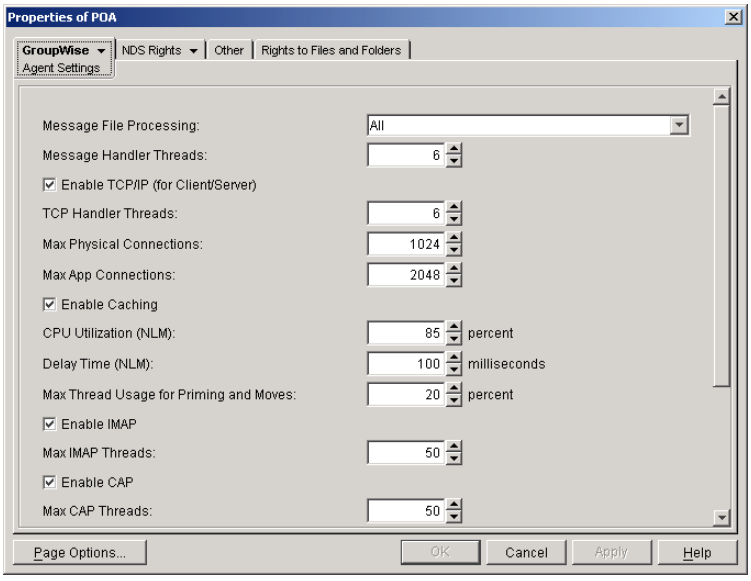
   You must use the hostnames ngwnameserver and ngwnameserver2. Any other hostnames are not recognized as GroupWise name servers.
8. Save your changes.

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.




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**

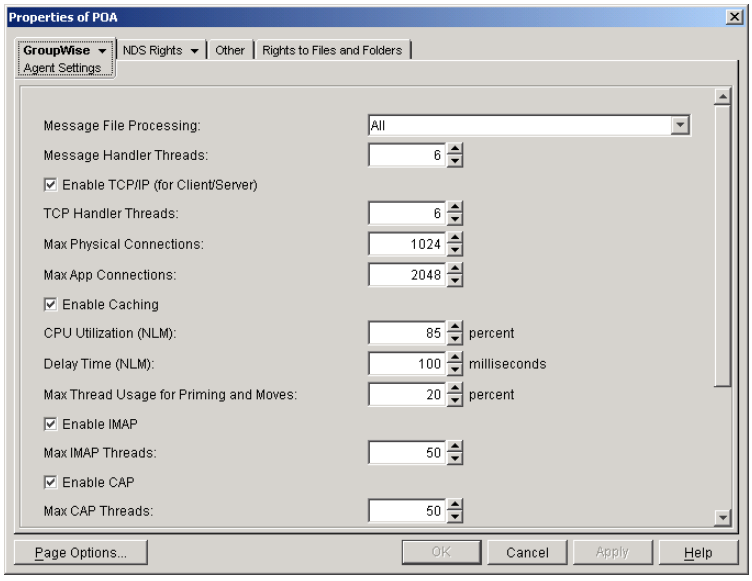
You can see whether IMAP is enabled on the Configuration page under the General Settings heading.

## 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.




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**

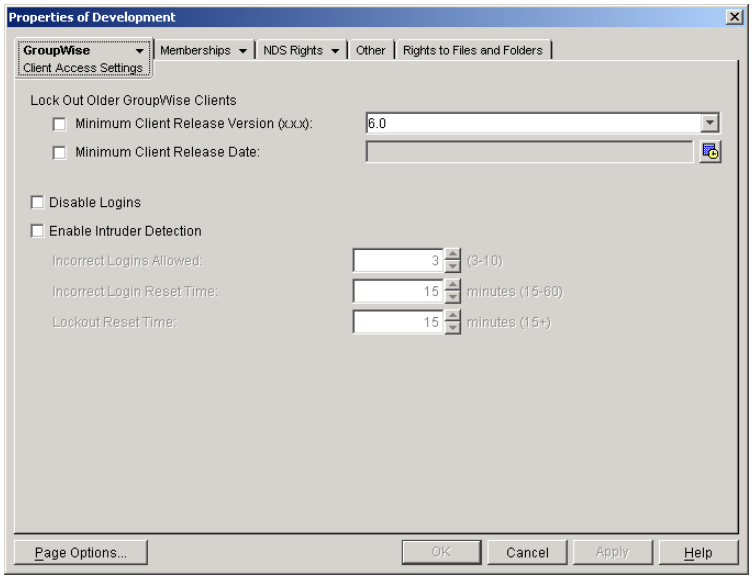
You can see whether CAP is enabled on the Configuration page under the General Settings heading.

## 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.




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

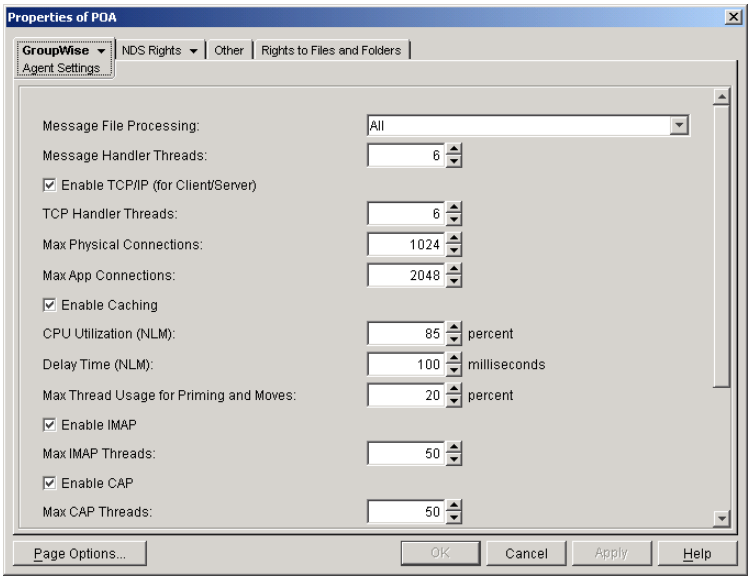
GroupWise client users have the option to download their GroupWise mailboxes to their workstations so they can work without being continuously connected to the network. This is called Caching mode. For more information, see “Caching Mode” on page 965.

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.




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.

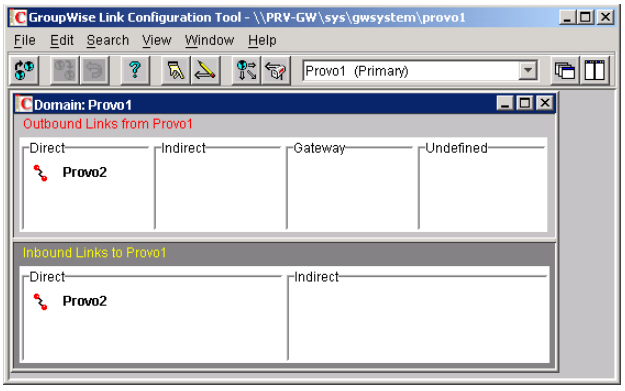
**POA Web Console**

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.

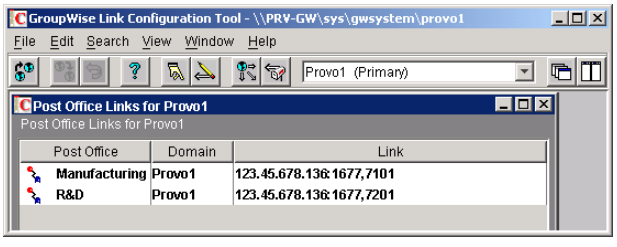
## Restricting Message Size between Post Offices

You can configure the POA to restrict the size of messages that users are permitted to send outside the post office.

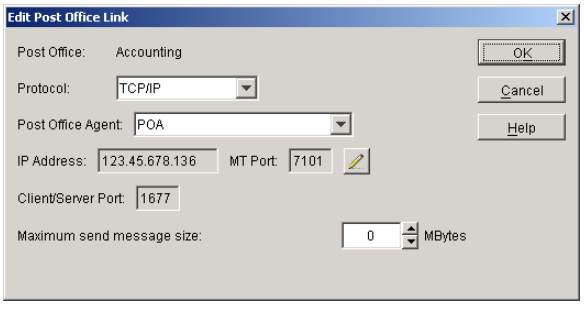
1. In ConsoleOne, click Tools > GroupWise Utilities > Link Configuration.




2. In the drop-down list, select the domain where the post office resides, then click Post Office Links.




3. Double-click the post office where you want to restrict message size.




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

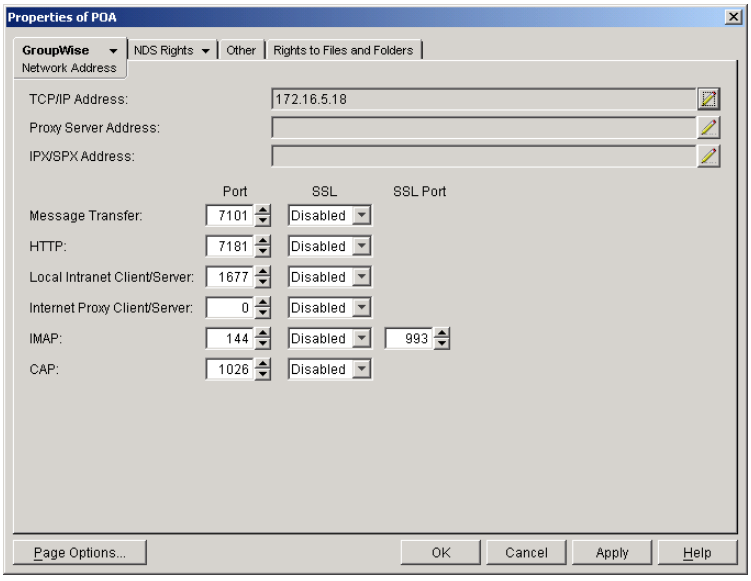
You can configure the POA in various ways to meet the security needs of the post office.

- "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

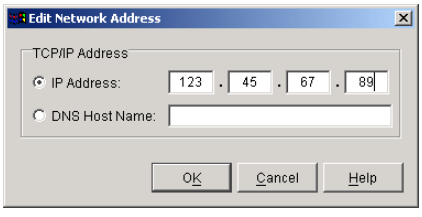
If the server where the POA runs is behind your firewall, you can link it to a proxy server in order to provide client/server access to the post office for GroupWise client users who are outside the firewall.

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.




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.




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.

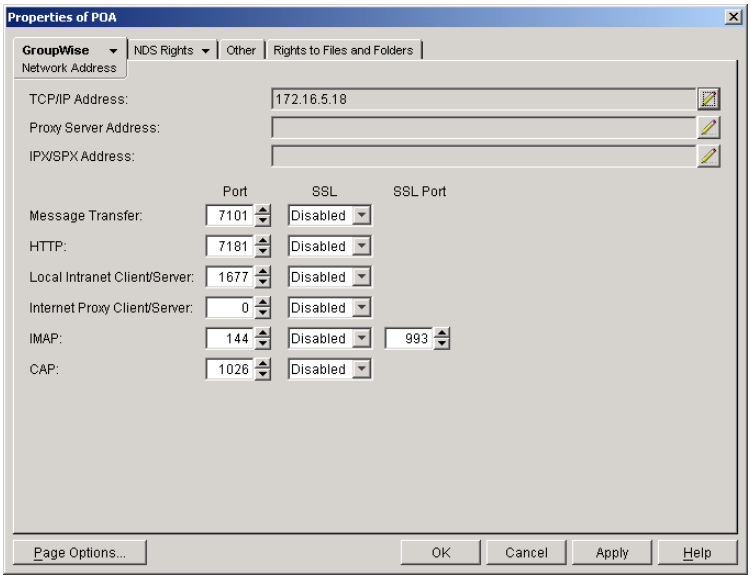
## Enhancing Post Office Security with SSL Connections to the POA

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.




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.

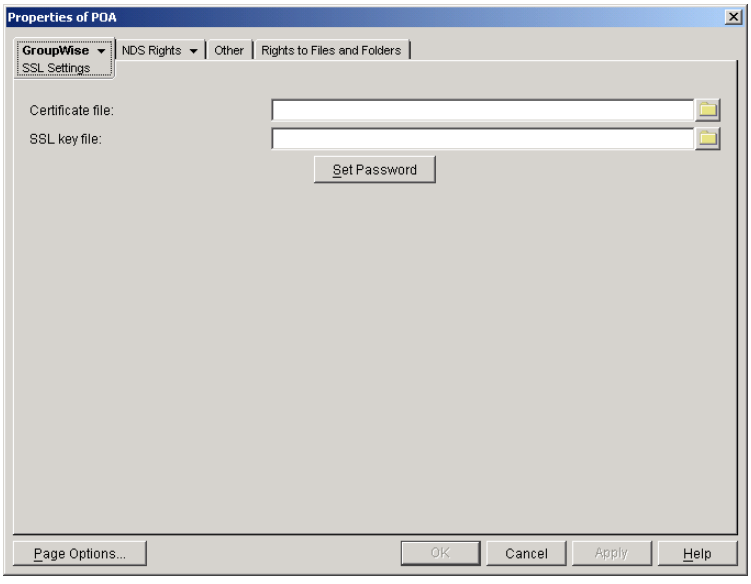
The MTA must also have SSL enabled for the connection to be secure. See "Enhancing Domain Security with SSL Connections to the MTA" on page 589. If the MTA does not have SSL enabled, the POA falls back to native GroupWise encryption.

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.




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.

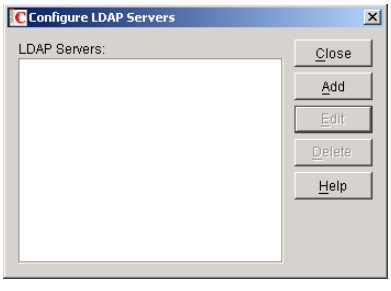
When you enable LDAP authentication, it is important to provide fast, reliable access to the LDAP directory because GroupWise client users cannot access their mailboxes until they have authenticated. The following sections provide instructions for configuring the POA to make the most efficient use of 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

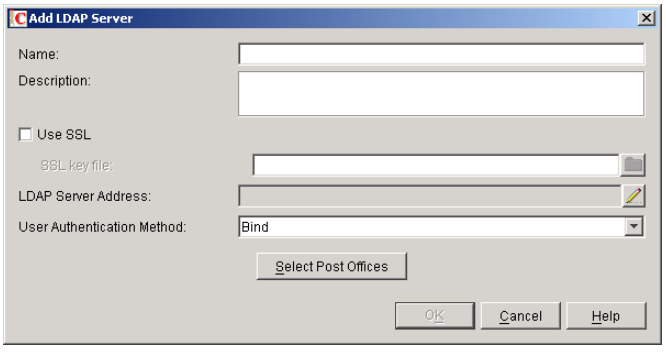
### Providing LDAP Server Configuration Information

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.



3 In the Name field, type the name by which you want the LDAP server to be known in your GroupWise system.

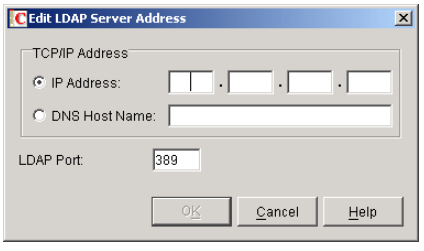
4 In the Description field, provide additional information about the LDAP server as needed.

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.




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

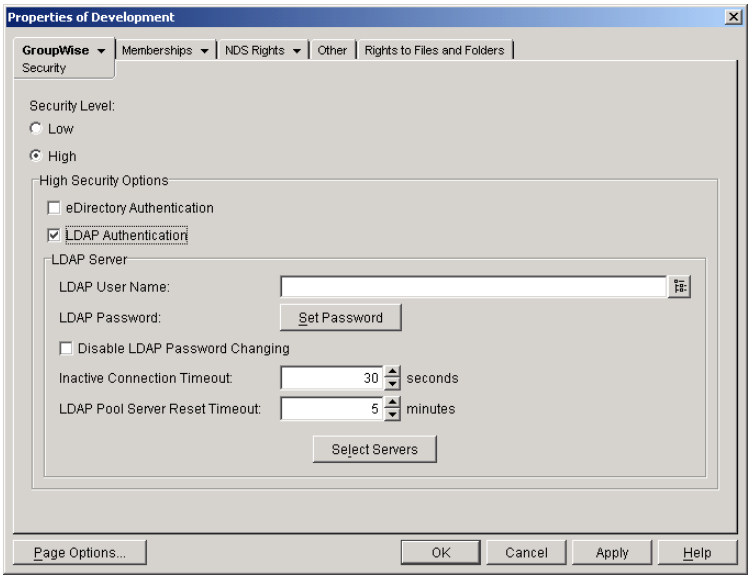
**Corresponding Startup Switches**
You could also use the /ldapipaddr, /ldapport, /ldapuserauthmethod, /ldapssl, and /ldapsslkey startup switches in the POA startup file to provide the LDAP server information.

### 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.




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.

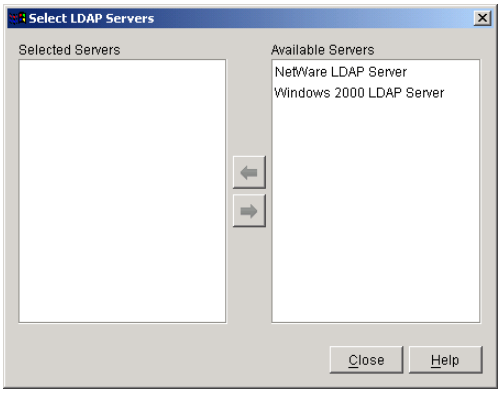
**POA Web Console**
You can see if LDAP is enabled on the Configuration page. Under the General Settings heading, click LDAP Authentication to view LDAP settings and change some of them for the current POA session.

### 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:

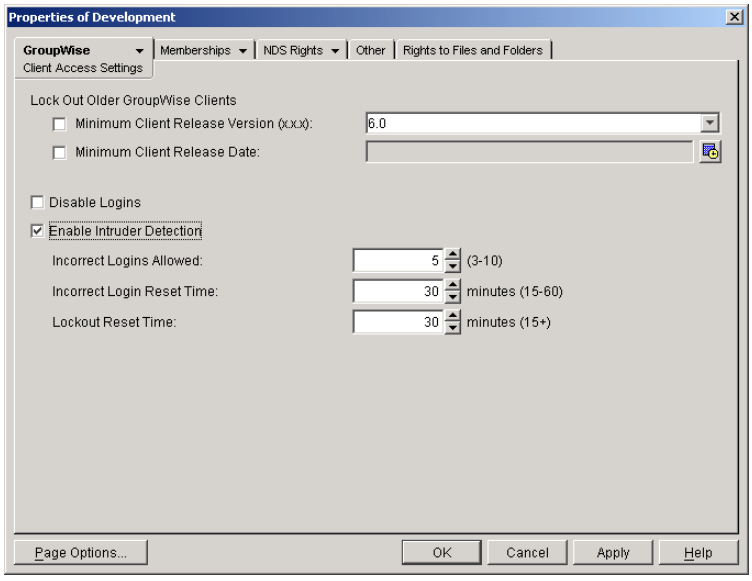
   /ldapipaddr-123.45.67.89 135.246.7.8 987.65.43.21

   **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.




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

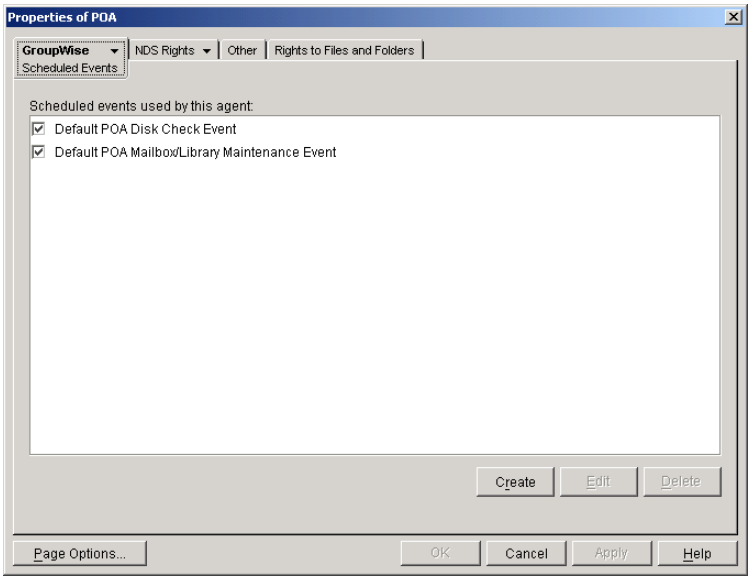
You can configure the POA to manage databases and disk space in the post office on a regular basis:



## Scheduling Database Maintenance

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.




The Scheduled Events page lists a pool of POA events available to all POAs in your GroupWise system.

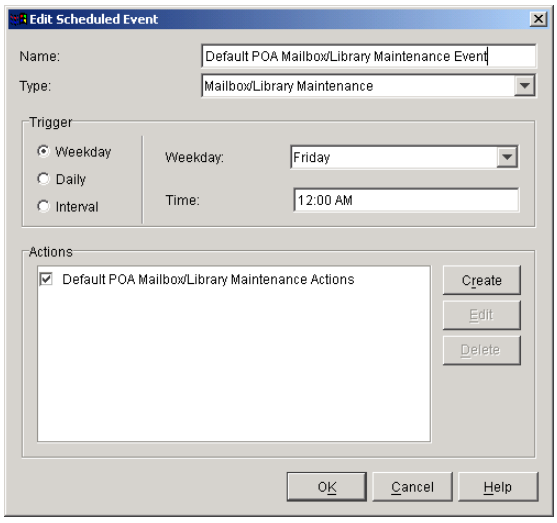
3. To modify the default database maintenance event, which would affect all POAs that have this database maintenance event enabled, select Default POA Mailbox/Library Maintenance Event, then click Edit.

   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.




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**<br>Structure<br>Index check<br>Contents<br>Collect statistics<br>Fix problems<br>Reset user disk space totals<br><br>**Analyze/Fix Library**<br>Verify library<br>Fix document/version/element<br>Verify document files<br>Validate security<br>Synchronize username<br>Reassign orphaned documents<br>Reset word lists | **Databases**<br>User<br>Message<br>Document<br><br>**Logging**<br>Log file<br>Verbose log level<br><br>**Results mailed to**<br>Administrator<br>Individual users<br><br>**Exclude**<br>Selected users<br><br>**Notification**<br>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**

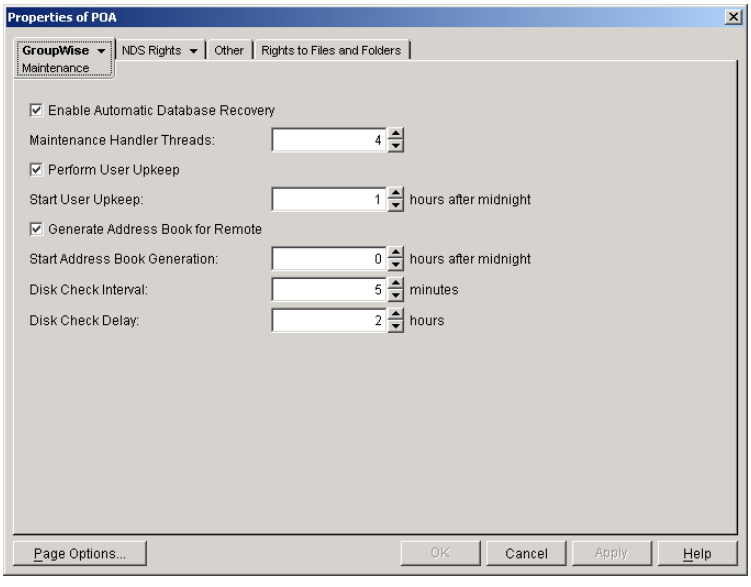
You can see what database maintenance events the POA is scheduled to perform at the bottom of the Configuration page.

## 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.




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.

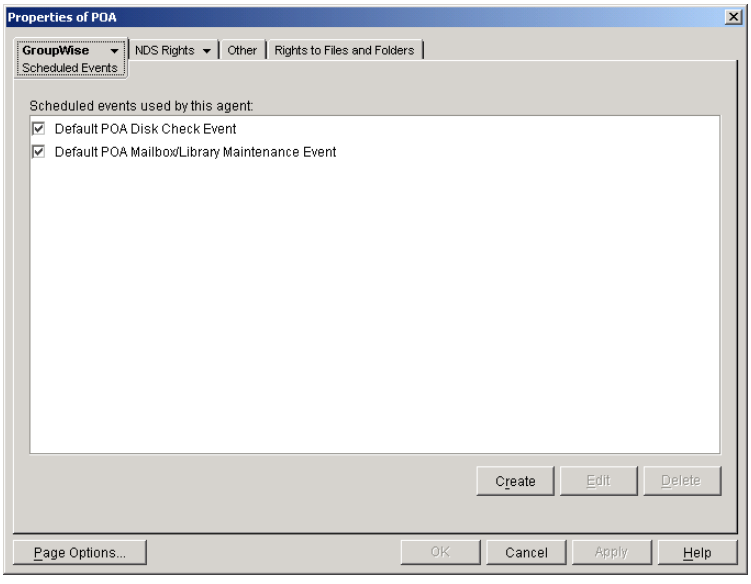
When a disk space problem is encountered, the time interval no longer applies until after the situation has been corrected. Instead, the POA continually checks available disk space to determine if it can restart message threads that have been suspended because of the low disk space condition.

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.



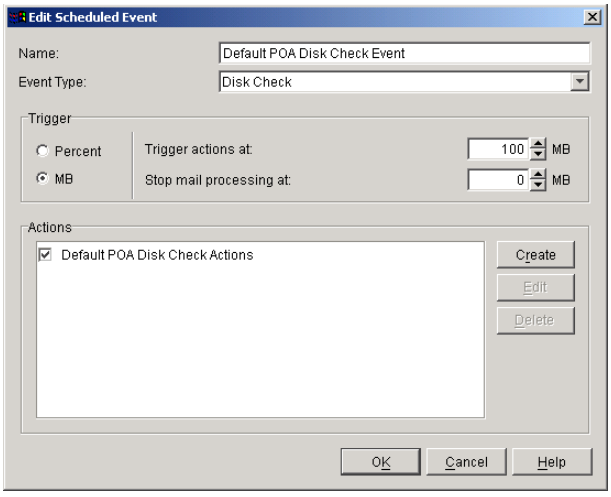

The Scheduled Events page lists a pool of POA events available to all POAs in your GroupWise system.

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.




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**<br>Reduce only<br>Expire and reduce<br>- Items older than<br>- Downloaded items older than<br>- Items larger than<br>- Trash older than<br>- Reduce mailbox to<br>- Reduce mailbox to limited size<br>Include<br>- Received items<br>- Sent items<br>- Calendar items<br>- Only backed-up items<br>**Archive/Delete Documents**<br>**Delete Activity Logs** | **Databases**<br>User<br>Message<br>Document<br>**Logging**<br>Log file<br>Verbose log level<br>**Results**<br>Administrator<br>Individual users<br>**Misc**<br>Support options<br>**Exclude**<br>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.

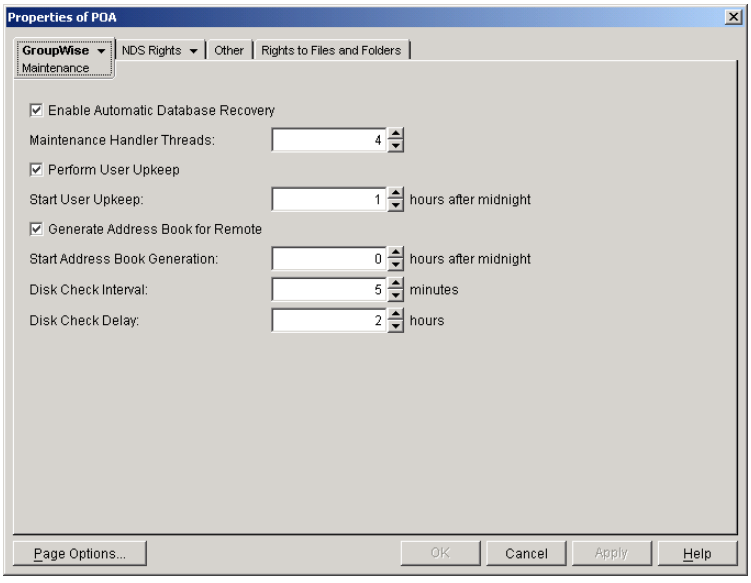
## Performing Nightly User Upkeep

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.




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:



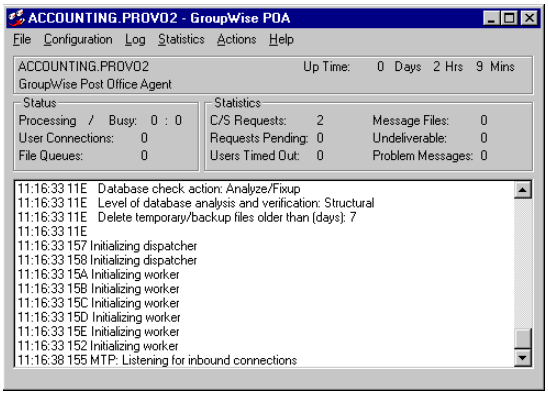
## Using the POA Agent Console

The following topics help you monitor and control the POA from the POA agent console:



### 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.



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.

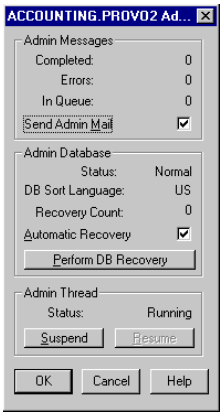
### Error Messages

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.




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.

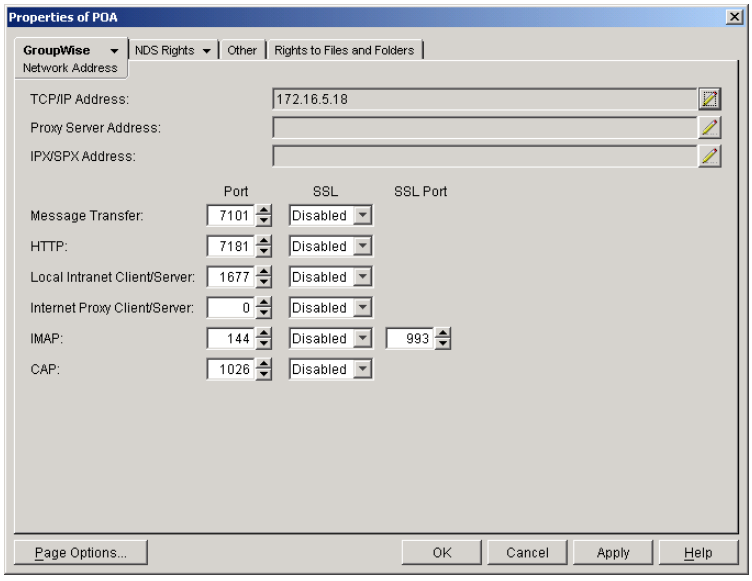
- “Setting Up the POA Web Console” on page 489
- “Accessing the POA Web Console” on page 491
- “Monitoring the POA from the POA Web Console” on page 492
- “Controlling the POA from the POA Web Console” on page 495

## 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.




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.

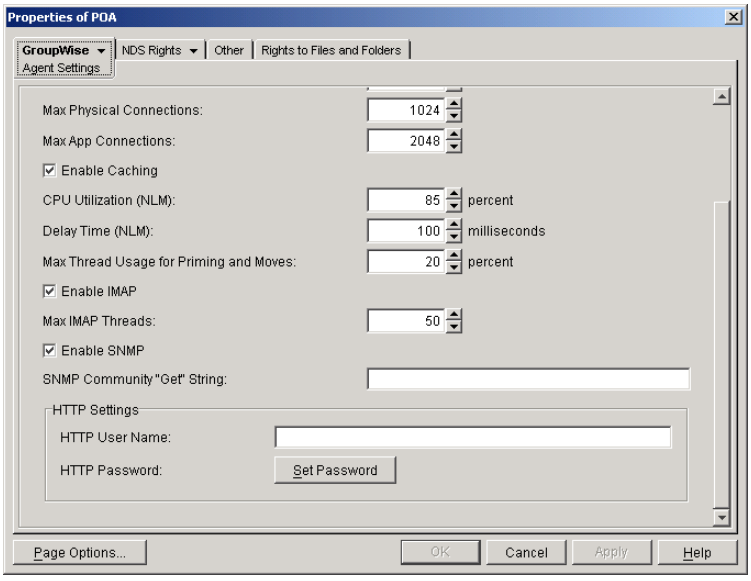
6 If you want to use an SSL connection for the POA Web console, select Enabled in the HTTP SSL drop-down list.

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.




**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**

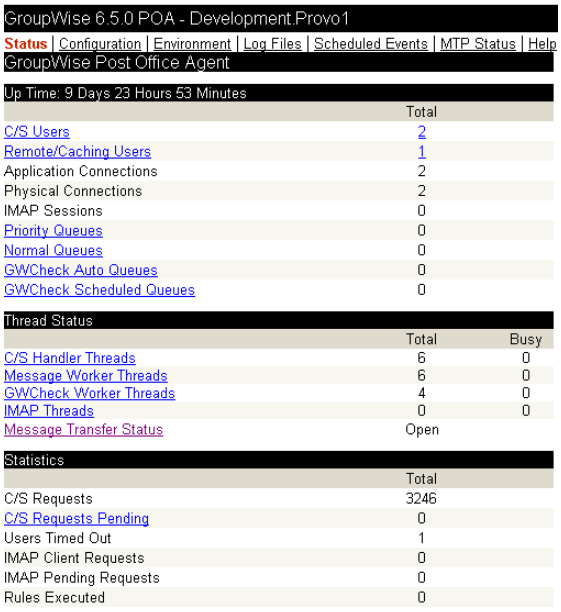
You could also use the /httpport, /httpuser, /httppassword, and /httpssl startup switches in the POA startup file to enable and secure the POA Web console. In addition, you can use the /httprefresh switch to control how often the POA refreshes the information provided to your Web browser.

## 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 |

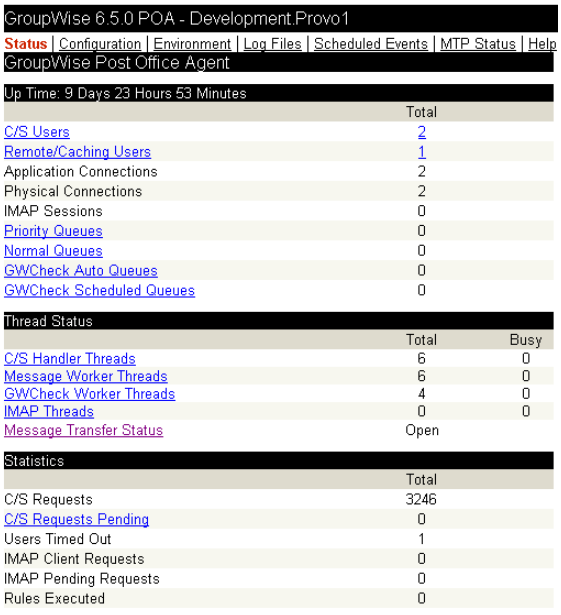
## Monitoring the POA from the POA Web Console

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

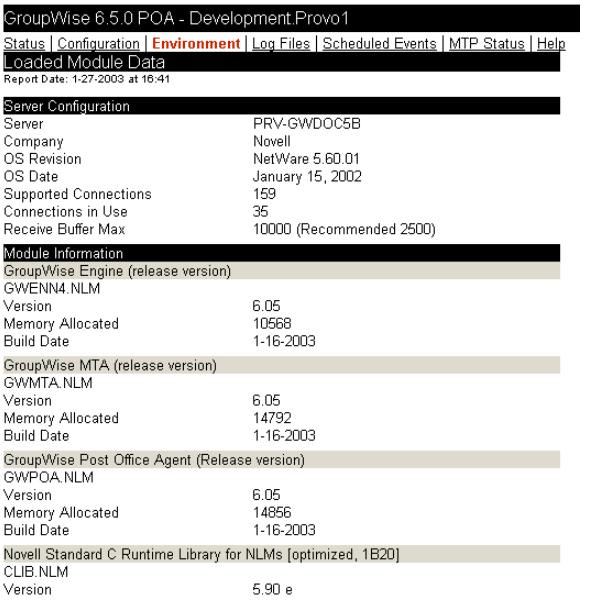
When you first access the POA Web console, the Status page is displayed. Online help on the Status page helps you interpret the status information being displayed.



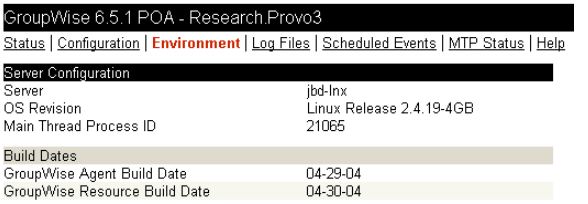

Click any hyperlinked status items for additional details. The status information is much the same as that provided at the POA agent console, as described in "Monitoring the POA from the POA Agent Console" on page 475.

### Checking the POA Operating System Environment

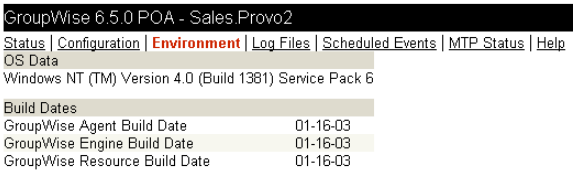
On the POA Web console menu, click Environment to display information about the operating system where the POA is running. On a NetWare server, the following information is displayed:




On a Linux server, the following information is displayed:

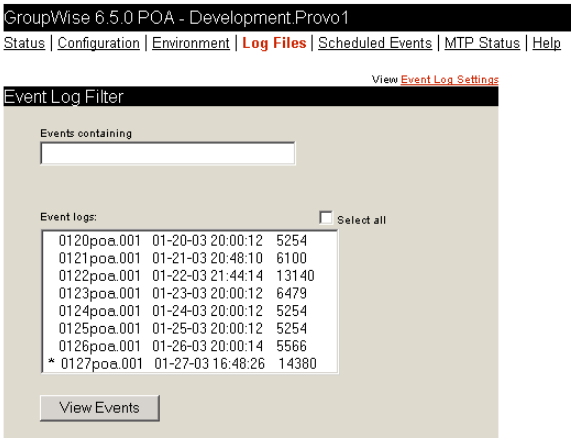



On a Windows server, the following information is displayed:




### Viewing and Searching POA Log Files

On the POA Web console menu, click Log Files to display and search POA log files.



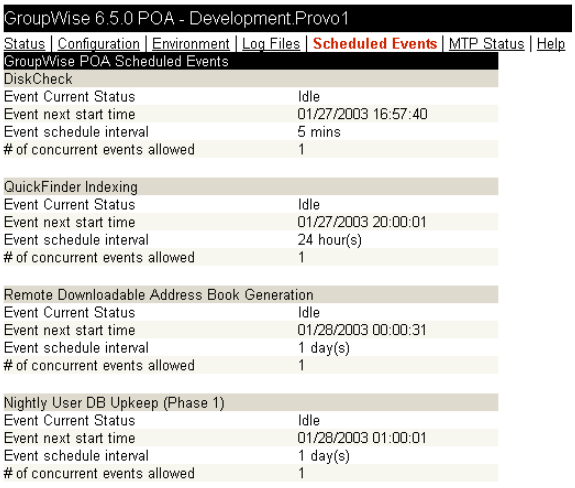

To view a particular log file, select the log file, then click View Events.

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

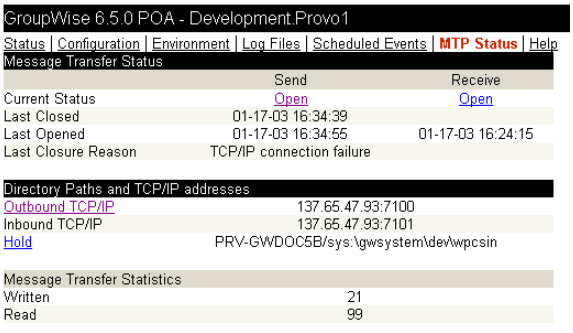
On the POA Web console menu, click Scheduled Events to view currently scheduled events and their status information.




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.




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.

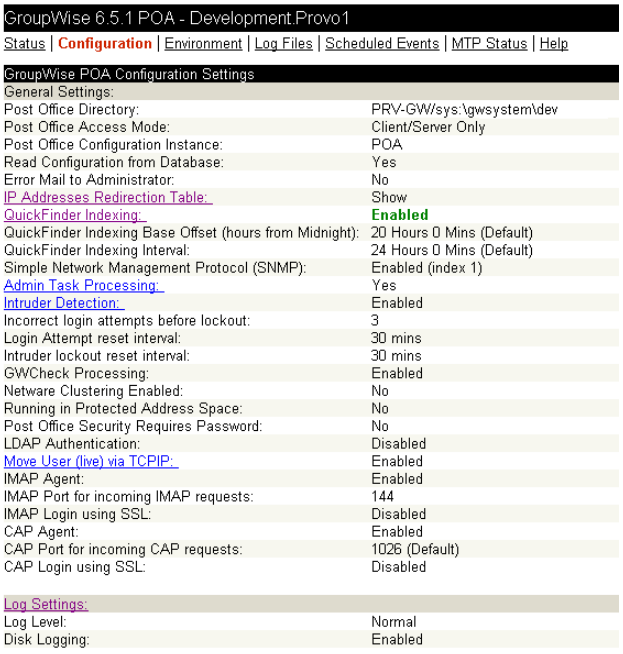
## Controlling the POA from the POA Web Console

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

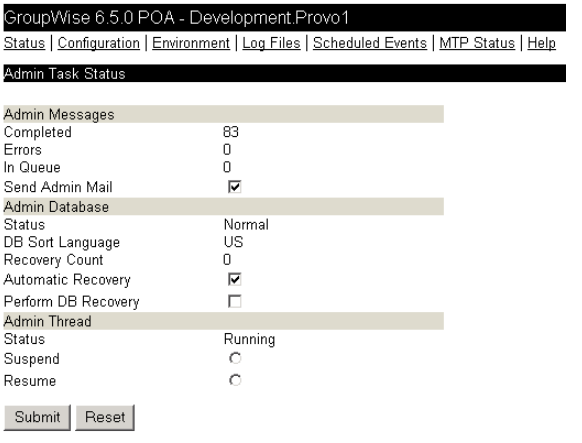
On the POA Web console menu, click Configuration. Online help on the Configuration page helps you interpret the configuration information being displayed.




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

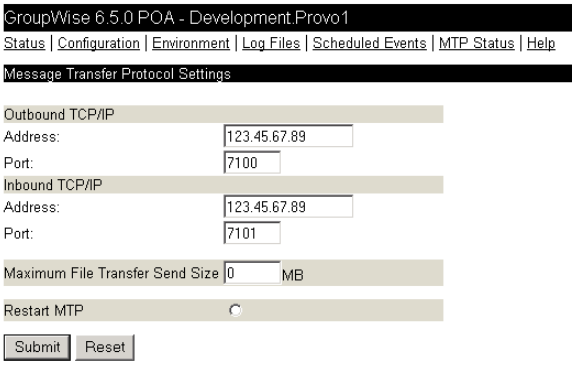
On the Configuration page, click Admin Task Processing.




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.




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

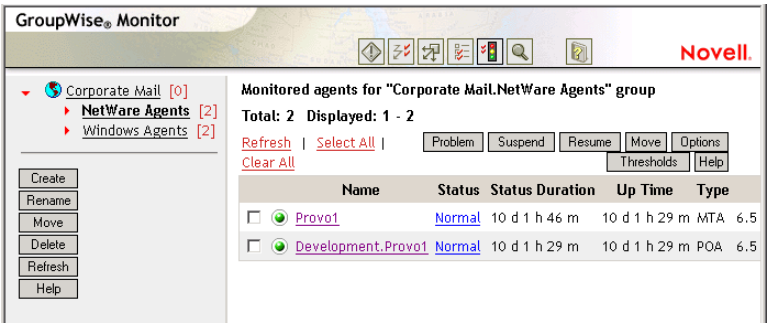
## Interpreting POA Log File Information

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.




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.

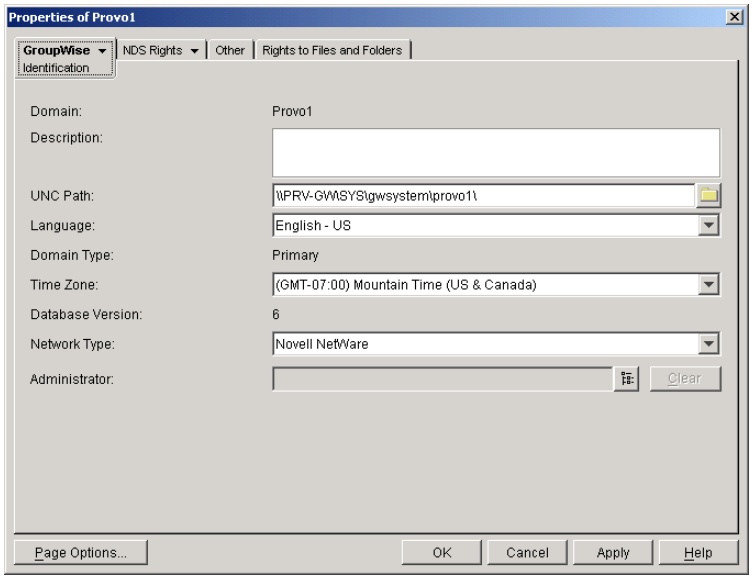
   ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

   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.




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

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

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

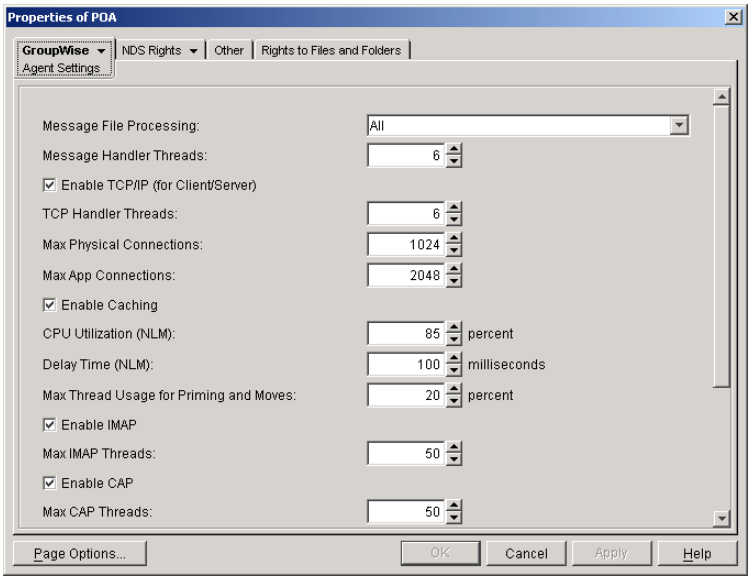
If the POA is configured with client/server processing enabled, it starts TCP handler threads to respond to current client/server requests, up to the number of threads specified by the TCP Handler Threads option. To respond to occasional heavy loads, the POA can increase the number of TCP handler threads 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.




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.

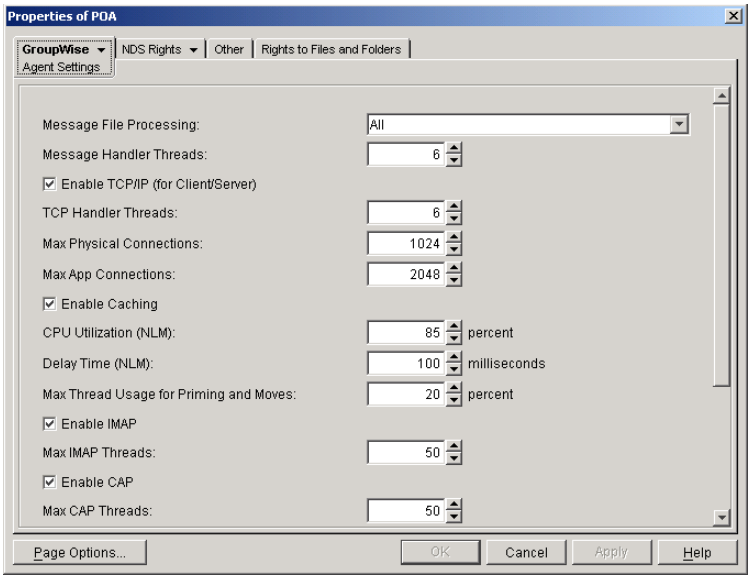
## Adjusting the Number of Connections for Client/Server Processing

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.




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.

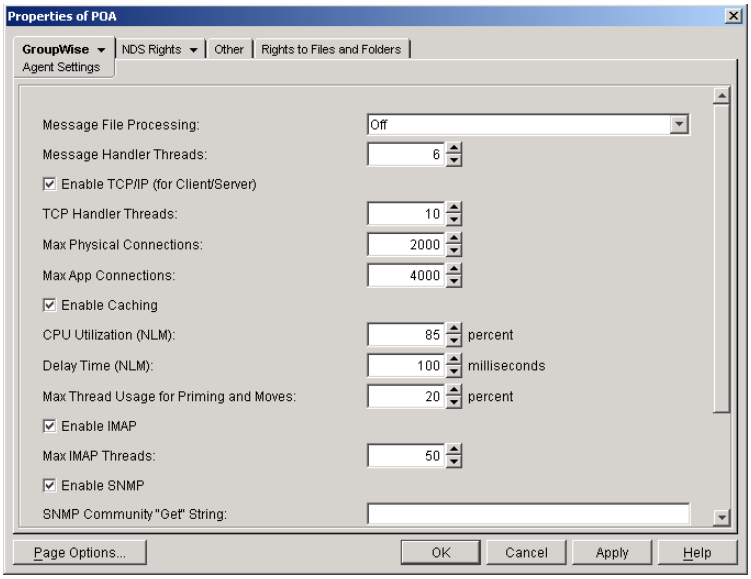
## Configuring a Dedicated Client/Server POA

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.




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

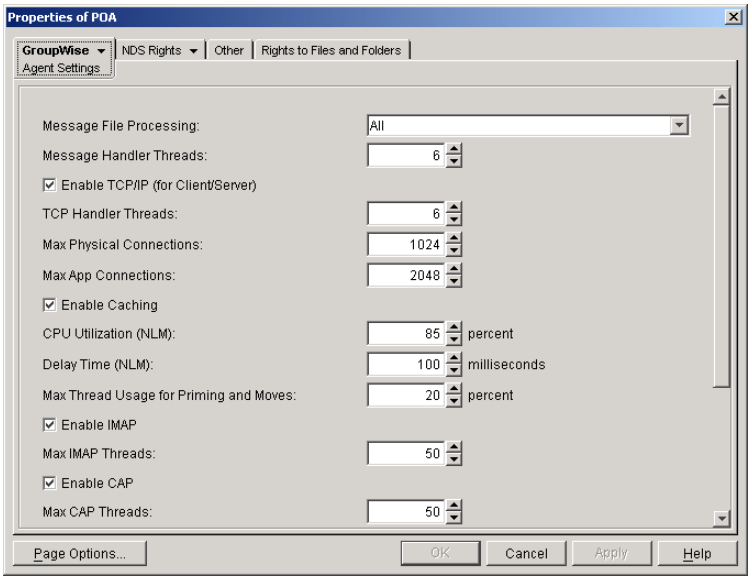
## Adjusting the Number of POA Threads for Message File Processing

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.




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.

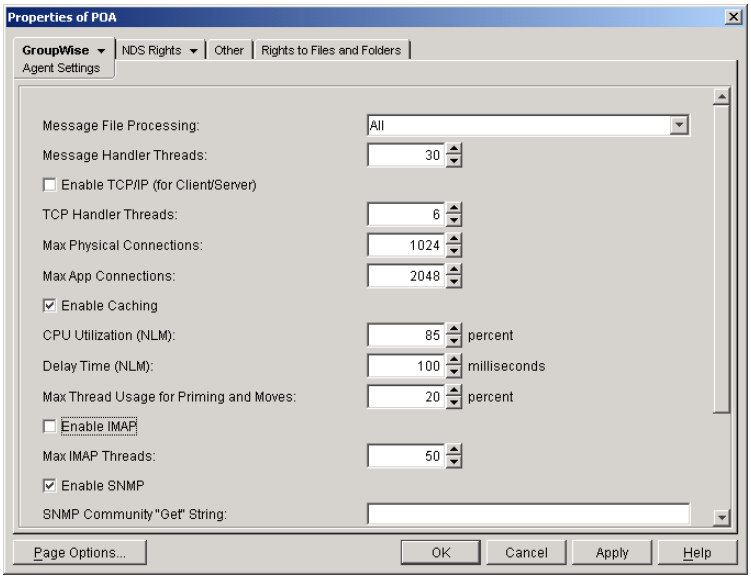
**POA Web Console**
The Status page helps you assess whether the POA is currently meeting the message file processing needs of the post office. Under the Thread Status heading, click Message File Processing Threads to display the workload and status of the message handler threads.

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.




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.

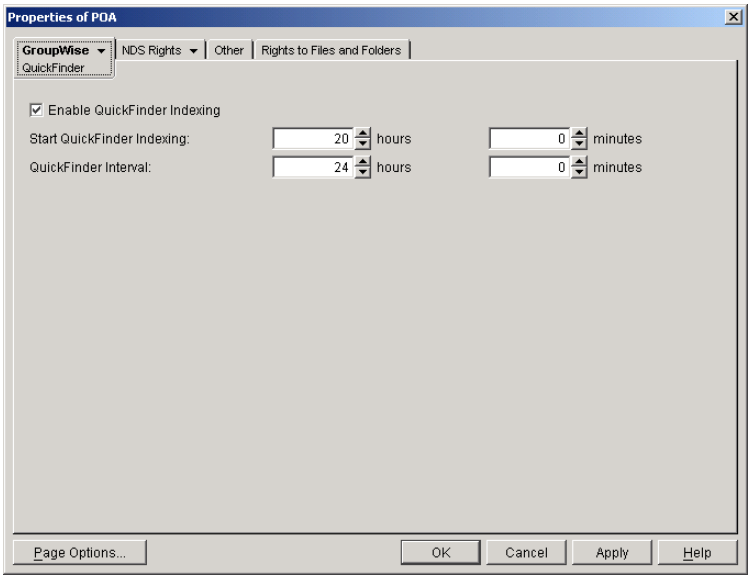
## Regulating Indexing

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.




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**

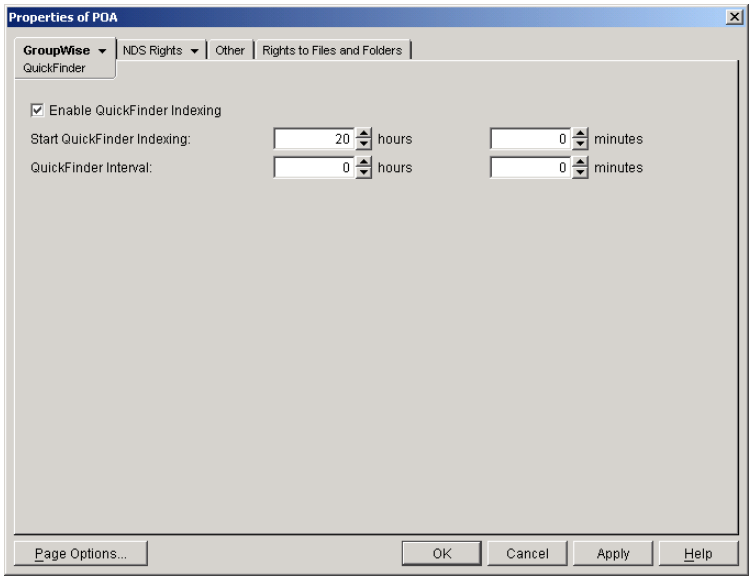
You can control indexing for the current POA session on the Configuration page. Under the General Settings heading, click QuickFinder Indexing. If indexing is currently in progress, you can check the status of the indexing process on the Scheduled Events page.

## 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.




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

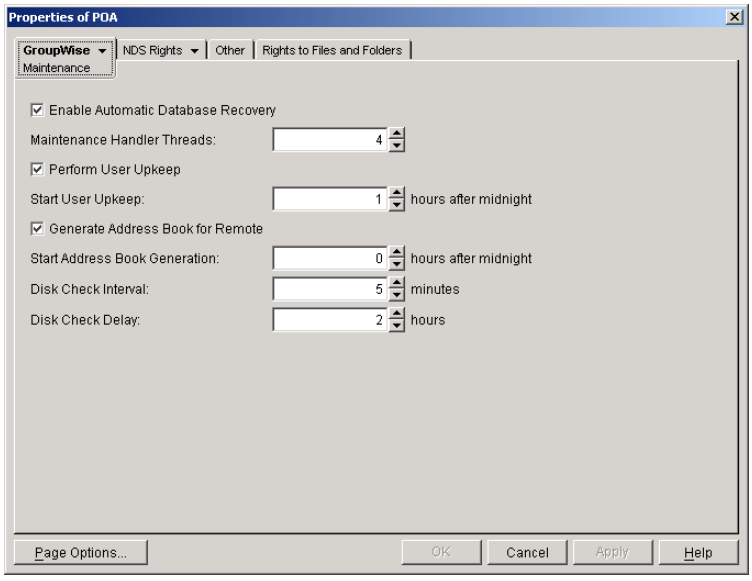
The POA by default performs a certain amount of database maintenance. In addition, you can create your own customized maintenance events as described in "Scheduling Database Maintenance" on page 467 and "Scheduling Disk Space Management" on page 469.

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.




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.

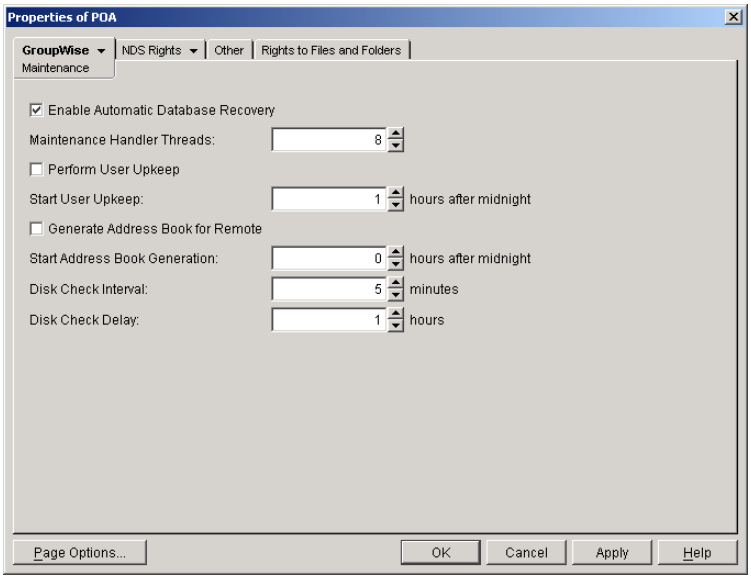
## Configuring a Dedicated Database Maintenance POA

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.




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.

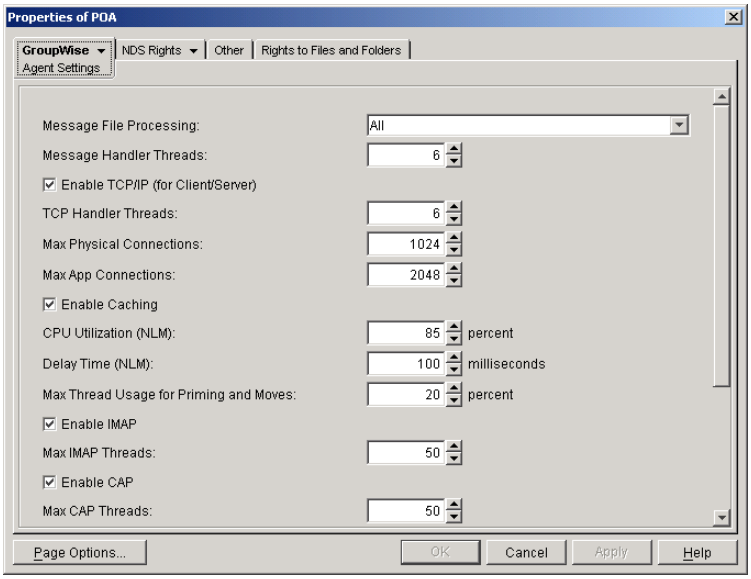
To determine the optimum utilization setting for your network, you must consider the following factors:

- 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.




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*<br>@*svr**vol**dir**file* | @[/*dir*/]*file* | @[*drive*:][*dir*\]*file*<br>@*svr**sharename**dir**file* |
| **Example:** | load gwpoa @sales.poa<br>load gwpoa @sys:\agt\sales.poa<br>load gwpoa @\\s2\sys\agt\sales.poa | ./gwpoa @../share/lnxpost.poa | gwpoa.exe @sales.poa<br>gwpoa.exe @d:\agt\sales.poa<br>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*<br>/certfile-*svr**vol**dir**file* | --certfile /*dir*/*file* | /certfile-[*drive*:]*dir**file*<br>/certfile-*svr**sharename**dir**file* |
| **Example:** | /certfile-\ssl\gw.crt<br>/certfile-server2\sys:\ssl\gw.crt<br>/certfile-\\server2\sys\ssl\gw.crt | --certfile /certs/gw.crt | /certfile-\ssl\gw.crt<br>/certfile-m:\ssl\gw.crt<br>/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*<br>/home-*svr**vol**dir* | --home */dir* | /home-[*drive*:]*dir*<br>/home-*svr**sharename**dir* |
| **Example:** | /home-\sales<br>/home-mail:\sales<br>/home-server2\mail:\sales<br>/home-\\server2\mail\sales | --home /gwsystem/sales | /home-\sales<br>/home-m:\sales<br>/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*<br>/keyfile-*svr**vol**dir**file* | --keyfile /*dir*/*file* | /keyfile-[*drive*:]*dir**file*<br>/keyfile-*svr**sharename**dir**file* |
| **Example:** | /keyfile-\ssl\gw.key<br>/keyfile-server2\sys:\ssl\gw.key<br>/keyfile-\\server2\sys\ssl\gw.key | --keyfile /certs/gw.key | /keyfile-\ssl\gw.key<br>/keyfile-m:\ssl\gw.key<br>/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<br>/ldapipaddr-server1 server2 | --ldapipaddr 172.16.5.19<br>--ldapipaddr server1 server2 | /ldapipaddr-172.16.5.20<br>/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.

# /ldappool*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:** | /ldappool*n*-*network_address* | --ldappool*n* *network_address* | /ldappool*n*-*network_address* |
| **Example:** | /ldappool1-172.16.5.18<br>/ldappool2-server1<br>/ldappool3-172.16.5.19 | --ldappool1 172.16.5.18<br>--ldappool2 server1<br>--ldappool3 172.16.5.19 | /ldappool1-172.16.5.18<br>/ldappool2-server1<br>/ldappool3-172.16.5.19 |

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*<br>/ldapsslkey-*svr**vol**dir**file* | --ldapsslkey /*dir*/*file* | /ldapsslkey-[*drive*:]*dir**file*<br>/ldapsslkey-*svr**sharename**dir**file* |
| **Example:** | /ldapsslkey-\ldap\gwkey.der<br>/ldapsslkey-server2\sys:\ldap\gwkey.der<br>/ldapsslkey-\\server2\sys\ldap\gwkey.der | --ldapsslkey /certs/gwkey.der | /ldapsslkey-\ldap\gwkey.der<br>/ldapsslkey-m:\ldap\gwkey.der<br>/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*<br>/ldapsslkeypool*n*-*svr**vol**dir**file* | --ldapsslkeypool*n*-/*dir*/*file* | /ldapsslkeypool*n*-[*drive*:]*dir**file*<br>/ldapsslkeypool*n*-*svr**sharename**dir**file* |
| **Example:** | /ldapsslkeypool4-\ldap\gwkey.der<br>/ldapsslkeypool4-svr2\sys:\ldap\gwkey.der<br>/ldapsslkeypool4-\\svr2\sys\ldap\gwkey.der | --ldapsslkeypool4 /certs/gwkey.der | /ldapsslkeypool4-\ldap\gwkey.der<br>/ldapsslkeypool4-m:\ldap\gwkey.der<br>/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*<br>/log-*svr**vol**dir* | --log /*dir* | /log-[*drive*:]*dir*<br>/log-*svr**sharename**dir* |
| **Example:** | /log-\agt\log<br>/log-\\server2\mail:\agt\log<br>/log-\\server2\mail\agt\log | --log /gwsystem/logs | /log-\agt\log<br>/log-m:\agt\log<br>/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.